Letao Zhang

Search this site

About me | Research | Teaching | Useful Links

Letao Zhang

Office: Math Tower 4-116

Email: first name.last name @stonybrook(dot)edu

Mailing Address:

Department of Mathematics

Stony Brook University

100 Nicolls Road

Stony Brook, NY 11794

Navigation

About me
Contact
Research
Teaching
Useful Links
Sitemap

Teaching >

MAT 311 Number Theory, Spring 2015

-- Some of the topics we will cover are: Congruences, quadratic residues, quadratic forms, continued fractions, Diophantine equations, number-theoretical functions, and properties of prime numbers.

Organizational Information

- Class schedule: TTh 2:30PM- 3:50PM, Physics P127, Spring 2015
- Textbook: *An Introduction to the Theory of Numbers* by I. Niven, H. S. Zuckerman, H. L. Montgomery
- Office Hour: TTh 12:30pm–1:30pm
- Math Learning Center: Math Learning Center, in Math Tower S-240A, is there for you to get help

Schedule, Homeworks, and Grades

- **Grading Policy**
  Homework = 50%
  Maximum of Midterm 1, Midterm 2, and Final Exam = 25%
  In class presentation = 25%

- *Your final letter grade will be curved following the performance of the whole class.*

- **Homeworks**
  - Homework sets can be found

    Schedule Notes and Homeworks

  - Homework will be assigned every Thursday and collected the following Tuesday in class.
  - Homework counts 50% of your total scores.
  - No late homework will be accepted. Instead, the lowest 3 homework grades will be dropped.

- **Exams**
  - Make sure that you can attend the exams at the scheduled times.
  - Make-ups will not be given.
  - If one midterm exam is missed because of a serious (documented) illness or emergency, the semester grade will be determined based on the balance of the work in the course.

  - Exam Arrangements

What	When	Where
Midterm 1	March 12 2015, In Class	Physics P127
Midterm 2	April 14 2015, In Class	Physics P127
Final Exam	May 18 2015 , 11:15am-1:45pm	Physics P127

University Statements

Disability Support Services (DSS) Statement
If you have a physical, psychological, medical or learning disability that may impact your course work, please contact Disability Support Services, ECC (Educational Communications Center) Building, room 128, (631) 632-6748. They will determine with you what accommodations, if any, are necessary and appropriate. All information and documentation is confidential. Students who require assistance during emergency evacuation are encouraged to discuss their needs with their professors and Disability Support Services. For procedures and information go to the following website

http://www.stonybrook.edu/ehs/fire/disabilities

Academic Integrity Statement

Each student must pursue his or her academic goals honestly and be personally accountable for all submitted work. Representing another person's work as your own is always wrong. Faculty are required to report any suspected instances of academic dishonesty to the Academic Judiciary. Faculty in the Health Sciences Center (School of Health Technology & Management, Nursing, Social Welfare, Dental Medicine) and School of Medicine are required to follow their school-specific procedures. For more comprehensive information on academic integrity, including categories of academic dishonesty, please refer to the academic judiciary website at:

http://www.stonybrook.edu/commcms/academic_integrity/index.html

Critical Incident Management Statement
Stony Brook University expects students to respect the rights, privileges, and property of other people. Faculty are required to report to the Office of Judicial Affairs any disruptive behavior that interrupts their ability to teach, compromises the safety of the learning environment, or inhibits students' ability to learn. Faculty in the HSC Schools and the School of Medicine are required to follow their school-specific procedures.

Your solution to each problem should be complete and be written in complete sentences where appropriate					
Lecture		**Date**	**Topics**	**Lecture Notes**	**Homeworks**
Lect 01	Tu	1/27/2015	Cancelled due to blizzard		Homework 01 Due 02/12
Lect 02	Th	1/29/2015	1.1 Instroduction to Number Theory, 1.2 Divisibility: b = aq + r	lecture 02	
Lect 03	Tu	2/3/2015	1.2 Divisibiliy: greatest common divisor, Euclidean Algorithm	lecture 03	
Lect 04	Th	2/5/2015	1.3 Primes	lecture 04	Homework 02 Due 02/19
Lect 05	Tu	2/10/2015	1.4 binomial coefficient	lecture 05	
Lect 06	Th	2/12/2015	2.1 Congruence (Introduction)	lecture 06	Homework 03 Due 2/24
Lect 07	Th	2/19/2015	2.1 Congruence 2.2 Slutions of Congruences	lecture 07	
Lect 08	Tu	2/24/2015	2.2 Solutions of Congruences, 2.3 The Chinese Remainder Theorem	lecture 08	Homework 04 Due 3/3
Lect 09	Th	2/26/2015	2.3 Chinese Remainder Theorem and Solving Polynomial Equations	lecture 09	
Lect 10	Tu	3/3/2015	2.4 Divisibility among polynomials and more Solving Polynomial Equations	Lecture 10	No homework
Cancelled	Th	3/5/2015	Cancelled due to blizzard	Cancelled due to blizzard	
Lect 11	Tu	3/10/2015	Review for Midterm I	Lecture 11	Homework 05 Due 3/24
Midterm 1	**Th**	**3/12/2015**	**Midterm 1: It will cover materials from Lect 01 to Lect 11**	**Midterm I**	
Lect 12	Tu	3/24/2015	Primitive roots and order of a mod m	Lecture 12	
Lect 14	Tu	3/31/2015	Primitive roots and order of a mod m	Lecture 14	Homework 06 Due 03/31
Lect 15	Th	4/2/2015	Quadratic Reciprocity	Lecture 15	Homework 07 Due 04/09
Lect 16	Tu	4/7/2015	Talks at Simons Center		
Lect 17	Th	4/9/2015	Jacobi Symbol	Lecture 17	HW 08 Practice midterm II (with solutions)
Midterm II	Tu	4/14/2015	**Midterm II: It will cover materials from Lect 01 to Lect 14 (mainly chapters after midterm I); However, materials covered after midterm I require knowledge throughout the semester**	Midterm II	
			Square Roots, Tonelli's Algorithm,		Homework 09

Lect 18	Th	4/23/2015	Number os consecutive paris of squares mod p	Lecture 18	Due 04/30
Lect 19	Th	4/30/2015	Cyclotomic Polynomial and Mod n==1	Lecture 19	Practice final

01/29/2015 / Thu. Number Theory. L0

physics . P127

- TTh. 2:30 ~ 3:50 pm.

- Textbook: An introduction to the theory of numbers,
  Ivan Niven, Herbert. Zuckerman.
  Hugh L. Montgomery.

- Grading:

  Homework 50% — { No late Homework. / lowest 3 sets will be dropped,

  Max (Mid 1, Mid 2, final) 25%

  ~~Final 25%~~

  presentation . 25%

- Exams:

  Mid 1: March 12. 2015. in class

  Mid 2: April 14 2015, in class

  Final : May 18 2015, 11:15 AM ~ 1:45 PM.
  (Location: To be Announced)

- letao.zhang@stonybrook.edu.

- www.math.sunysb.edu/~lz7/

01/29/2015. ~~Thea~~ Number Theory, lecture 02.

· Introduction

- Objects we study: Integers: $\cdots -2, -1, 0, 1, 2, 3, \cdots$

  We denote the set of all integers by $\mathbb{Z}$

  $$\mathbb{Z} := \{\cdots -5, -4, -3, -2, -1, 0, 1, 2, \cdots\}$$

- Properties of $\mathbb{Z}$:

1. Divisibility.

$\boxed{eg}$: An integer is divisible by 2 if and only if it ends with an even number.

$2 \nmid 365$ $\qquad 2 \mid 366 \cdots$

$\boxed{eg}$: An integer is divisible by 3 if and only if ~~it ends with an~~ the sum of its digits is divisible by 3

- $78 \qquad 7+8=15 \qquad 3 \mid 15$ & thus $3 \mid 78$
- $77 \qquad 7+7=14 \qquad 3 \nmid 14$ & thus $3 \nmid 77$

$\boxed{eg}$: An integer is divisible by 5 if and only if it ends with 5 or 0

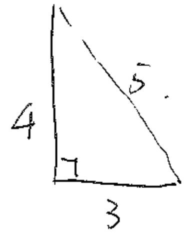
- 10: $\quad 5 \mid 10$ as 10 ends w/ 0
- $1111\boxed{5}$ $\quad 5 \mid 11115$. as 11115 ends w/ 0

? How abou 4 ?

study in this course.

2 Solutions to multivariable polynomials:

$\boxed{\text{eg}}$:



$3^2+4^2=5^2$.

<u>Question</u>: Does the equation $x^2+y^2=z^2$ has any solution? How many?

- $x=3,\ y=4,\ z=5$ is one solution
- Actually, it has infinitely many solutions.

<u>Question</u>: Algorithmatically, we can always run computer program to check for solutions

$\boxed{\text{eg}}$:

for $x=[-1000,\ 1000]$

$y=[-1000,\ 1000]$

$z=[-1000,\ 1000]$

test if $x^2+y^2=z^2$ for each pairing

Why we need number theory?

(1): Computer cannot tell you there are NO solutions

(2): Computer cannot tell you there are infinitly many solutions.

In this class, we will introduce ways of finding $\boxed{\text{int.}}$ solutions.

for polynomials of a few variables

eg : $x^3+y^3=z^3$, $x^4+y^4=z^4$ have no integer solutions

Famous "Conj": Fermat's last Theorem:

$x^n+y^n=z^n$ has NO positive integer solutions for all $n>2$.

Note: this was still a conjecture by the time our textbook was written

---

Andrew Wiles

proved Fermat's Conjecture (or last Theorem)

June 23. ~~1~~993 (1994)

Technique: complex analysis, "Torus", Galois Rep.

Story of Fermat's last theorem (1601 ~ 1665)

French Mathematician sets problem & then solves them. Jots down in the margin of a book that he has a proof, but can't be bothered to write down the proof itself. Frenchmen dies, son discovers marginal note, publishes it, and the rest of the world starts trying to figure out the proof of Fermat's Last theorem. Everyone fails, until a boy (10-year-old) starts working on the problem in 1963. Roughly 30-years later he comes up w/ a proof

but he made a mistake, Damn! He's embarrassed & humiliated, (4)
but undaunted he sets down to work again and ...

3 Prime Numbers.

Defn: A prime is a natural number that cannot be factored into two smaller natural numbers ~~___~~.

$\boxed{\text{eg}}$: $2 = 2 \cdot 1$ prime

$3 = 3 \cdot 1$ prime

$4 = \boxed{2 \cdot 2} = 4 \cdot 1$ product of 2 natural numbers smaller than 4.

$5 = 5 \cdot 1$ prime

Theorem: There are infinitely many prime numbers (To be proven in this course).

? what ~~do~~ prime numbers look like?

properties like:
except for 2, all prime numbers are odd.

Goldbach Conjecture (1742) Every EVEN integer greater than 2 is the sum of two primes, as in the example:

$4 = 2 + 2 \quad 6 = 3 + 3 \quad 8 = 3 + 5 \ \cdots$

$100 = 29 + 71 \ \cdots$

unsolved! still! We will NOT try to solve this in class!

Also called: binary conjecture

Alternatively: Theorem: Every odd integer (>5) is the sum of 3 primes.

$7 = 2+2+3$, $9 = 2+2+5$
$= 3+3+3$ } NOT unique

$11 = 2+2+7$ . . . .
$= 3+3+5$

NOTE: Solving Goldbach conjecture will easily indicate above Theorem.

[proof]: Given an odd ~~prime~~ number m, $m > 5$.

then $m-3$ is even and $m-3 > 2$.

By Goldbach conjecture, every even number (>2) is the sum of two primes.

thus: $m-3 = P_1 + P_2 \Rightarrow m = \underbrace{3 + P_1 + P_2}_{\text{sum of 3 primes}}$ ∎

In this class, we will try to solve problems involving prime numbers. Be prepared to write proofs

---

In number theory, it's easy to make conjectures, but it is sometimes ~~very~~ hard to prove the conjecture.

(To disprove, you just need one counter example!)

eg: "I" conjecture that, for every natural number n, n^2+n+7 is a prime number.

Easy to find: for $n=1$, $1^2+1+7=9$ NOT prime

So $n=1$ is a counter example to my conjecture.

1.2. Divisibility:

Defn. An integer b is divisible by an integer a, NOT zero, if there is an integer x such that $b=ax$, and we write $a|b$. In case b is NOT divisible by a, we write $a \nmid b$.

$a|b$ means: a divides b; a is a divisor of b, b is a multiple of a,

eg: $6=2\cdot 3 = 1\cdot 6$

2, 3, 1, 6 are all divisors of 6.

we have: $2|6$, $1|6$, $3|6$, $6|6$

5 is NOT a divisor of 6. then $5 \nmid 6$;

eg: For 0, every integer (NONE zero) divides 0

So $n|0$ for all nonzero integer n.

$\boxed{eg}$: 0 is NEVER a divisor of any integer.

$\underline{\underline{so}}$ "$0 \mid n$" is WRONG $\boxed{\text{always}}$:

<u>Observation</u>: If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$

<u>i.e.</u> a divisor of a number is always less than or equal to the number.

<u>Theorem 1.1</u>:

(1) $a \mid b$ implies $a \mid bc$ for any integer c, $\left(2 \mid 6 \overset{eg}{\Rightarrow} 2 \mid 6 \cdot 5 \right)$

(2) $a \mid b$ and $b \mid c$, imply $a \mid c$, $(2 \mid 8,\ 8 \mid 24 \Rightarrow 2 \mid 24)$

(3) $a \mid b$ and $a \mid c$, imply $a \mid (bx + cy)$ for any integers x, y.
$(3 \mid 6,\ 3 \mid 27 \Rightarrow 3 \mid 6-27,\ 3 \mid -21)$

(4): $a \mid b$ and $b \mid a$, imply $a = b$ or $a = -b$ (write $a = \pm b$)
$(2 \mid -2,\ -2 \mid 2 \Rightarrow 2 = -(-2) = 2)$

(5): $a \mid b$, $a > 0$, $b > 0$, imply $a \leq b$; $(10 \mid 100,\ 10 < 100)$

(6): If $m \neq 0$, $a \mid b$ implies and is implied by $ma \mid mb$.

$$\left(\begin{array}{l} 7 \mid 56 \Rightarrow 2 \cdot 7 \mid 2 \cdot 56 \\ 8 \mid 24 \ \text{i.e.}\ 2 \cdot 4 \mid 2 \cdot 12 \Rightarrow 4 \mid 12. \end{array} \right)$$

[proof]: (1): $a \mid b$. by <u>defn</u>: $b = ax$ for some int. x.

then: $bc = axc$. $\underline{\underline{so}}$ $bc = a \cdot (xc) \Rightarrow a \mid bc$.

(2) - -

Theorem 1.2 The division algorithm. Given any integers a. b, with $a>0$ there exists unique integer q and r, such that

$$b = qa + r, \quad 0 \le r < a.$$

If $a \nmid b$, then r satisfies the stronger inequalities

$$0 < r < a.$$

---

eg: Given two integers: 7, 30, write $30 = q \cdot 7 + r$ where $0 \le r < 7$.

Consider the arithmetic progression. ($b=30$, $a=7$.)

$\cdots, b-3a, b-2a, b-a, b, b+a, b+2a, \cdots$

$30 - 5 \cdot 7 = -5 < 0$

$30 - 4 \cdot 7 = 2 \in [0, 7)$ $\quad 30 = 4 \cdot 7 + 2$

$30 - 3 \cdot 7 = 9 > 7$

eg: Given $a=5$, $b=35$. write b as $q \cdot a + r$ where $0 \le r < a$.

We know. $5 \mid 35$, $\quad \underset{q \cdot 5 + r}{35 = 7 \cdot 5 + 0}$ $\quad r = 0 \in [0, 5]$

[proof]: Consider the arithmetic progression: ⑨

If $b-a>0$ consider

$b-2a$

$b-3a$

$b-4a$

$\vdots$

If $b-a<0$ consider

$b+a$

$b+2a$

$b+3a$

$\vdots$

select the smallest nonnegative member & denote it by r.

Thus by definition r satisfies the inequalities of theorem

uniqueness. if we have $b=q_1a+r_1$, $b=q_2a+r_2$

step 1 Show. $r_1=r_2$,

Assume $r_1<r_2$ then $0<r_2-r_1<a$.

$\Rightarrow$: $b-b=(q_1-q_2)a+r_1-r_2$ $\Rightarrow$: $r_2-r_1=(q_1-q_2)a$

$\Rightarrow a \mid r_2-r_1$ contradiction to $0<r_2-r_1<a$.

Thus $r_1 = r_2 = r$

$\Rightarrow$ $b = q_1 a + r$ $\qquad$ $b = q_2 a + r$

$\Rightarrow$ $q_1 = q_2$

Division w/ remainder Given $a, b \in \mathbb{Z}$, $a > 0$, $\exists ! q, r \in \mathbb{Z}$

<u>Such that</u> $b = aq + r$, $0 \le r < a$

($\exists$ — symbol for there exists , $\exists!$ — symbol for there exists unique)

$\boxed{eg}$: $a = +10 \quad b = -3$ write $b = qa + r$. $0 \le r < a$

$-3 = 10q + r$. $\quad q = -1 \quad r = 7$

Greatest common divisor

<u>Definition</u>. The integer $\underline{\underline{a}}$ is a <u>common divisor</u> of b and c in case $a | b$ and $a | C$.

<u>Note</u>. There is only a finite number of common divisors of b and c if at least one of b and c is NOT $\emptyset$.

<u>Definition</u>: <u>Greatest common divisor</u> of b and c, denoted by (b, C), is the largest among their common divisors. (assume $b \ne 0$ or $c \ne 0$)

$\boxed{eg}$. Find common divisors of 306 and 45.

<u>From the smallest</u>: 1 — 306 and 45 are relatively prime

Defn: We say two integers $\underline{a}$ and $\underline{b}$ are relatively prime in case $(a,b) = 1$.

eg: Find common divisors of 81, 54.

divisors of 81: 1, 3, 9, 27, 81

divisors of 54: 1, 2, 3, 6, 9, 18, 27, 54

} largest $\underline{\underline{27}}$

eg: Find G-common divisors (GCD) of 81, 54, 9

Greatest common divisors of 3 numbers:

$$((81,54),9) = (27,9) = 9$$

Definition: Common divisors of integers $b_1, \cdots, b_n$ (at least one of them is zero) are collections of number c, such that $c \mid b_1, \cdots, c \mid b_n$

Definition: Greatest common divisors of integers $b_1, \cdots, b_n$ are the largest of collections of numbers divide all b_i's

Thm 1.3: If g is the greatest common divisor of b and c, then $\exists$ integers x_0, y_0, such that $g = (b,c) = bx_0 + cy_0$

Note Not unique: $GCD(2,4) = 2$. $2 = -2 + 4$, $2 = 3 \cdot 2 - 4$

13

Another proof

Recall that Given $a, b \in \mathbb{Z}$, $a > 0$, $\exists q, r \in \mathbb{Z}$ S.T. $b = aq + r$

Proof. Let set $S = \{b + ka : k \in \mathbb{Z}, b + ka \geq 0\}$.

$$S \text{ is nonempty: } \begin{cases} b > 0 & \text{then } b + 0a \in S \\ b < 0 & \text{then adding } a \text{ enough times makes it positive} \end{cases}$$

We can make this rigorous by another application of WOP - since S is nonempty, it has a smallest element $r = b + ka$ for some k. Setting $q = -k$ results in $r = b - qa$. $r \geq 0$ because its in S, and $r < a$ because if not, then $b + (k-1)a$ would be smallest element in S instead ($\lightning$). ■

Note: $a | b$ iff $r = 0$

(Definition): If a and b are not both 0, then $\gcd(a, b)$ or (a, b) is the **greatest common divisor** of a and b

Theorem 2. *Let $g = (a, b)$. Then $\exists\, v_0, y_0 \in \mathbb{Z}$ such that $g = ax_0 + by_0$.*

Proof. Let set $S = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$, and assume a, b not both 0.

$$S \text{ is nonempty (wlog, assume } a \neq 0\text{): } \begin{cases} a > 0, a \in S \\ a < 0, -a \in S \end{cases}$$

Since S is nonempty, it has a smallest element $g = ax + by$. To prove theorem, show that $g | a$, $g | b$, and g is largest common divisor (if another common divisor d, then $d | g$).

$g | a$ ***by contradiction (assume*** $g \nmid a$***).***

$$\begin{aligned} a &= gq + r, 0 < r < g \\ r &= a - gq \\ &= a - q(ax + by) \\ &= a(1 - qx) - b(qy) \\ &\Rightarrow r \in S, \text{but } r < g, \text{ so } g \text{ isn't smallest } \lightning \end{aligned}$$

g is largest common. If $d | a$ and $d | b$, then $d | ax + by = g$

Since $g | a$, $g | b$, and g is largest common divisor, then g is gcd of a, b. ■

(Definition) Co-Prime, Relatively Prime: If $(a, b) = 1$, then a and b are **co-prime**, or **relatively prime**.

4

Corollary 3. *If* $(a, m) = 1$ *and* $(b, m) = 1$, *then* $(ab, m) = 1$

Proof.

$$\begin{aligned} 1 &= ax + my, ax = 1 - my \\ 1 &= bx' + my', bx' = 1 - my' \\ abxx' &= (1 - my)(1 - my') \\ &= 1 - my - my' + m^2yy' \\ &= 1 + m(-y - y' + myy') \\ 1 &= ab(xx') + m(y + y' - myy') \end{aligned}$$

■

Corollary 4. *If* $c|ab$ *and* $(c, a) = 1$, *then* $c|b$

Proof.

$$\begin{aligned} (a, c) = 1 &\Rightarrow 1 = ax + cy \\ &\Rightarrow b = abx + bcy \\ c|ab,\ c|bc &\Rightarrow c|(abx + bcy) = b \end{aligned}$$

■

Thm 1.5

Greatest common divisor g of $b_1, \cdots, b_n$ can be expressed as:

$$g = (b_1, \cdots, b_n) = \sum_{j=1}^{n} b_j x_j$$

[proof]: Note GCD of b_1, b_2 can be expressed as:

$$g_{12} = y_1 b_1 + y_2 b_2$$

GCD of $b_1\ b_2\ b_3$ is the GCD: $((b_1, b_2), b_3)$

i.e. $(g_{12}, b_3) \Rightarrow c_{12} g_{12} + c_3 b_3$

$$\Rightarrow c_{12}(y_1 b_1 + y_2 b_2) + c_3 b_3$$

$$= \underline{c_{12} y_1}\, b_1 + \underline{c_{12} y_2}\, b_2 + \underline{c_3}\, b_3$$

Induction: Assume for $n-1$ integers we have GCD expression: $g' = c_1 b_1 + \cdots + c_{n-1} b_{n-1}$

For n integers: $(b_1, \cdots, b_n) = ((b_1, \cdots, b_{n-1}), b_n)$

$= (g', b_n) \leftarrow$ case of 2 integers

Thus (g', b_n) has expression: $d_1 g' + d_2 b_n$

$$d_1(c_1 b_1 + \cdots + c_{n-1} b_{n-1}) + d_2 b_n$$

$$(b_1, \cdots, b_n) = d_1 c_1 b_1 + d_2 c_2 b_2 + \cdots + d_2 b_n$$

5

[redacted]

Euclidean Algorithm, Primes

Euclidean gcd Algorithm - Given $a, b \in \mathbb{Z}$, not both 0, find (a, b)

- Step 1: If $a, b < 0$, replace with negative
- Step 2: If $a > b$, switch a and b
- Step 3: If $a = 0$, return b
- Step 4: Since $a > 0$, write $b = aq + r$ with $0 \leq r < a$. Replace (a, b) with (r, a) and go to Step 3.

Proof of correctness. Steps 1 and 2 don't affect gcd, and Step 3 is obvious. Need to show for Step 4 that $(a, b) = (r, a)$ where $b = aq + r$. Let $d = (r, a)$ and $e = (a, b)$.

$$\begin{aligned} d = (r, a) &\Rightarrow d|a,\ d|r \\ &\Rightarrow d|aq + r = b \\ &\Rightarrow d|a, b \\ &\Rightarrow d|(a, b) = e \\ e = (a, b) &\Rightarrow e|a,\ e|b \\ &\Rightarrow e|b - aq = r \\ &\Rightarrow e|r, a \\ &\Rightarrow e|(r, a) = d \end{aligned}$$

Since d and e are positive and divide each other, are equal. ∎

Proof of termination. After each application of Step 4, the smaller of the pair (a) strictly decreases since $r < a$. Since there are only finitely many non-negative integers less than initial a, there can only be finitely many steps. (Note: because it decreases by at least 1 at each step, this proof only shows a bound of $O(a)$ steps, when in fact the algorithm always finishes in time $O(\log(a))$ (left as exercise)) ∎

To get the linear combination at the same time:

		43	27
	43	1	0
1	27	0	1
1	16	1	-1
1	11	-1	2
2	5	2	-3
5	1	-5	8
	0	$\Rightarrow 1 = -5(43) + 8(27)$	

Goal: Find GCD of 43, 27

		43	27	
	43	1	0	
① → 1	27	0	1	
② → 1	16	1	$\cancel{-7}$ -1	← $16 = 43 - 1 \cdot 27$
③ → 1	11	① − ② -1	2	$11 = 27 - 16$
④ → 2	5	② − ③ 2	-3	← $5 = 16 - 11$
5	1	③ − 2·④ -5,	8	$1 = 11 - 2 \cdot 5$
	0	$1 = -5 \cdot 43 + 8 \cdot 27$		

Thm 1.6. For any positive integer m, $(ma, mb) = m(a,b)$

[proof]: (ma, mb) = least positive value of $max + mby$

$= m$ (least positive value of $ax+by$)

$= m(a,b)$ ∎

- Defn. Common Multiple: The integers $a_1, \cdots, a_n$ (ALL None zero), have a common multiple b if $a_i | b$ for $i = 1, 2, \cdots, n$. (common multiples exist & there are infinitely many) eg. $a_1 \cdots a_n$, $(a_1 \cdots a_n)^2$, $\cdots$

- Defn. The least of all positive common Multiples is called the least common multiple, denoted by $[a_1, \cdots, a_n]$.

Thm:
$$[a_1, \cdots, a_n] = \frac{|a_1 a_2 \cdots a_n|}{(a_1, \cdots, a_n)^{n-1}}$$

[eg]:
$$[a, b] = \frac{|ab|}{(a,b)}$$

Note let $g = (a, b)$. then $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$

eg: Find GCD of 963 and 657

$963 = 1 \cdot 657 + 306$

$657 = ? \cdot 306 + ? = 2 \cdot 306 + 45$

$306 = ? \, 45 + ? = 6 \cdot 45 + 36$

$45 = ? \, 36 + ? = 1 \cdot 36 + 9$

$36 = 4 \, (9) + 0$

$306 = (963 - 657)$

$45 = 657 - 2 \cdot 306 = 657 - 2 \cdot (963 - 657)$

$= 3 \cdot 657 - 2 \cdot 963$

$36 = 306 - 6 \cdot (3 \cdot 657 - 2 \cdot 963)$

$= (963 - 657) - 6 \, (3 \cdot 657 - 2 \cdot 963)$

$= 13 \cdot 963 - 19 \cdot 657$

$9 = 45 - 36$

$= 3 \cdot 657 - 2 \cdot 963 - (13 \cdot 963 - 19 \cdot 657)$

$= 22 \cdot 657 - 15 \cdot 963$

Thm 1.11 Repeated Application of division Algorithm: Given $b, c > 0$

$b = c \, q_1 + r_1$ ($r_1 < c$)

$c = q_2 \, r_1 + r_2$ ($r_2 < r_1$)

$r_1 = q_3 \, r_2 + r_3$ ($r_3 < r_2$)

$\vdots$

$r_{j-1} = r_j \, q_{j+1} + 0$ (Finite steps).

$r_1 = b - q_1 c$

$r_2 = c - q_2 r_1$

$r_3 = r_1 - q_3 r_2$

expressed in terms of b, c.

eg: Show that $GCD\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$

If $d = \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)$

then $d \mid \frac{a}{(a,b)}$, $d \mid \frac{b}{(a,b)}$

$\Rightarrow d \mid a$. $d \mid b \Rightarrow d\cdot(a,b) \mid a$

$d\cdot(a,b) \mid b$

Since (a,b) is GCD of a and b,

d has to be 1

eg Evaluate $(n, n+1)$ $n \in \mathbb{Z}_+$

cases $n=1$. $(1,2)=1$

$n=2$ $(2,3)=1$

$n=3$ $(3,4)=1$

Guess $(n, n+1)=1$.

assume $(n, n+1) = d > 1$

$n = d n_1$ ①

$n+1 = d n_2$ ②

② − ①

$\Rightarrow 1 = d(n_2 - n_1)$

$\Rightarrow d \mid 1$ (contradiction to $d>1$)

$\Rightarrow d=1$

eg1 Find values of x, y s.t.

$$93x - 81y = 3$$

Consider GCD 93 and 81

			93	81	
1		93	1	0	
2	1	81	0	1	
3	6	12	1	-1	1 − 2
4	1	9	-6	$+7$	2 − 6·3 =
	3	3	7	-8	3 − 4
		0			

$$\boxed{3 = 7\cdot 93 - 8\cdot 81}$$

eg: Show that $4 \nmid n^2+2$ for any integer n

[proof]: $4 \mid n^2+2 \Rightarrow$ $n^2+2 = 4q$

$n^2 = 4q-2 = 2(2q-1)$

$\Rightarrow$ $2 \mid n^2 \Rightarrow n^2$ is even

$\Rightarrow$ n is even $\Rightarrow$ $2 \mid n \Rightarrow 4 \mid n^2$

$\Rightarrow$ $4 \mid 2(2q-1) \Rightarrow 2 \mid 2q-1$ contradiction

1.3 Primes.

Defn 1.5 An integer $P>1$ is called a prime number, or a prime, in case there is no divisor d of p satisfying $1<d<P$.

An integer $a>1$ is NOT a prime, it is called a composite number.

$2, 3, 5, 7, \cancel{9}, 11, 13, \cancel{15}, 17, 19, \cancel{21}$

Thm 1.15 If prime P, $P \mid ab$, then $P \mid a$ or $P \mid b$.

[pf]. If $p \nmid a$, then $(p, a)=1 \Rightarrow p \mid b$

(We proved before if $c \mid ab$ & $(b, c)=1$, then $c \mid a$)

Thm 1.16 The fundamental Theorem of Arithmetic (or unique factorization theorem).

Every positive integer can be ~~fact~~ written as a product of primes (possibly with repetition) and any such expression is unique up to a permutation of the prime factors.

(eg: $18 = 2 \cdot 3 \cdot 3 = 3 \cdot 2 \cdot 3 = 2 \cdot 3^2$)

Existence: (by contradiction)

Let S be the set of integers, having NO prime factorization

1 & primes $\notin S$

Let n be the smallest in S.

n is NOT prime $\Rightarrow n = n_1 n_2$, $1<n_i<n$

Since $n_i \notin S$ (n is smallest) $\Rightarrow$, n_i have prime fact —

then $n = n_1 n_2$ has prime fact. —

[uniqueness]: Assume two factorizations: $p_1 \cdots p_r = q_1 \cdots q_s$

then $p_i \mid q_1 \cdots q_s \Rightarrow \exists j$ $\boxed{\text{s.t.}}$ $p_i \mid q_j$

Since p_i & q_j are both primes, $p_i = q_j$

WLOG, $p_1 = q_1$

By induction $\Rightarrow$ two factorizations agree ∎

We write the prime factorization of a positive integer as:

$$n = \prod_p p^{\alpha(p)} \qquad \alpha(p) := \#\text{ of prime } p \text{ in the factorization}$$

- GCD $(a,b) = (a,b) = \prod_p p^{\min(\alpha(p), \beta(p))}$; $[a,b] = \prod_p p^{\max(\alpha(p), \beta(p))}$

where $a = \prod_p p^{\alpha(p)}$ & $b = \prod_p p^{\beta(p)}$

$\boxed{\text{eg}}$: $a = 108 \qquad b = 540$

then $a = 2^2 3^3 \qquad b = 2^2 3^3 \cdot 5^1$

$= 2^2 3^3 5^0 \qquad = 2^2 3^3 5^1$

$$GCD(108, 540) = 2^{\min(2,2)} 3^{\min(3,3)} 5^{\min(0,1)}$$

$$= 2^2 3^3 5^0 = 2^2 3^3$$

$$[108, 540] = 2^{\max(2,2)} \cdot 3^{\max(3,3)} 5^{\max(0,1)}$$

$$= 2^2 3^3 5^1$$

Thm 1.17 (Euclid) There are infinitely many primes.

[proof] (By contradiction) finitely many. $P_1 \cdots P_n$

let $n = P_1 \cdots P_n + 1$.

n has prime factorization. $\Rightarrow n = \prod_{i=1}^{n} P_i^{\alpha(P_i)}$ finitely many).

However. $n \pmod{P_i} \equiv 1$ ⋈

▣.

True or False

X (1): If $(a,b)=(a,c)$ then $[a,b]=[a,c]$
$(2,4)=(4,6)$, $[2,4]=4$, $[4,6]=12$

✓ (2): If $(a,b)=(a,c)$ then $(a^2,b^2)=(a^2,c^2)$
$\prod p^{\max(\alpha(p),\beta(p))}$

✓ (3) If $(a,b)=(a,c)$ then $(a,b)=(a,b,c)$
$(a,b)=((a,b),b)=((a,c),b)=(a,c,b)$

✓ (4) p-prime & $p|a$, and $p|a^2+b^2 \Rightarrow p|b$
($a^2+b^2 \equiv 0\ (p)$ $p|a \Rightarrow a(p)=0 \Rightarrow b^2 \equiv 0\ (p) \Rightarrow p|b^2 \Rightarrow p|b$)

✓ (5) p-prime & $p|a^7$, then $p|a$

HW △ (6) If $a^3|c^3$, then $a|c$

✓ (7): If $a^3|c^2$, then $a|c$

HW △ (8) If $a^2|c^3$, then $a|c$

✓ (9) If p is a prime, $p \mid (a^2+b^2)$ & $p \mid (b^2+c^2)$
then $p \mid a^2-c^2$

a

X (10). p-prime & $p \mid a^2+b^2$ & $p \mid b^2+c^2$, then $p \mid a^2+c^2$

$$\left(5 \mid 2^2+4^2 \ ,\ 5 \mid 4^2+3^2 \right)$$

✓ (11): If $(a,b)=1$, then $(a^2, ab, b^2)=1$

$$\left(p \mid (a^2, ab, b^2) \Rightarrow p \mid a^2 \Rightarrow p \mid a \quad \Rightarrow p \mid (a,b) \right.$$
$$\Rightarrow p \mid b^2 \Rightarrow p \mid b$$

HW Δ (12) $[a^2, ab, b^2] = [a^2, b^2]$

HW Δ (13): $b \mid a^2+1 \Rightarrow b \mid a^4+1$ another counter eg.

$$\left(5 \mid 3^2+1 \ ,\ 5 \nmid 3^4+1 \right)$$

✓ (14). If $b \mid (a^2-1)$ then $b \mid (a^4-1)$

HW Δ (15): $(a,b,c) = \left((a,b), (a,c) \right)$

Lecture 3
Binomial Coefficients, Congruences

$n(n-1)(n-2)\dots 1 = n! =$ number of ways to order n objects.

$n(n-1)(n-2)\dots(n-k+1) =$ number of ways to order k of n objects.

$\frac{n(n-1)(n-2)\dots(n-k+1)}{k!} =$ number of ways to pick k of n objects. This is called a

(Definition) Binomial Coefficient:

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

Proposition 10. *The product of any k consecutive integers is always divisible by $k!$.*

Proof. wlog, suppose that the k consecutive integers are $n-k+1, n-k+2\dots n-1, n$. If $0 < k \le n$, then

$$\frac{(n-k+1)\dots(n-1)(n)}{k!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

which is an integer. If $0 \le n < k$, then the sequence contains 0 and so the product is 0, which is divisible by $k!$. If $n < 0$, then we have

$$\prod_{i=1}^{k}(n-k+i) = (-1)^k \prod_{i=0}^{k-1}(-n+k-i)$$

which is comprised of integers covered by above cases. ∎

We can define a more general version of binomial coefficient

(Definition) Binomial Coefficient: If $\alpha \in \mathbb{C}$ and k is a non-negative integer,

$$\binom{\alpha}{k} = \frac{(\alpha)(\alpha-1)\dots(\alpha-k+1)}{k!} \in \mathbb{C}$$

Theorem 11 (Binomial Theorem)**.** *For $n \ge 1$ and $x, y \in \mathbb{C}$:*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Proof.

$$(x+y)^n = \underbrace{(x+y)(x+y)\dots(x+y)}_{n \text{ times}}$$

To get coefficient of $x^k y^{n-k}$ we choose k factors out of n to pick x, which is the number of ways to choose k out of n $\blacksquare$

Theorem 12 (Generalized Binomial Theorem)**.** *For* $\alpha, z \in \mathbb{C}, |z| < 1$,

$$(1+z)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} z^k$$

Proof. We didn't go through the proof, but use the fact that this is a convergent series and Taylor expand around 0

$$f(z) = a_0 + a_1 z + a_2 z^2 \ldots \quad a_n = \left.\frac{f^{(k)}(z)}{k!}\right|_{z=0}$$

$\blacksquare$

Pascal's Triangle: write down coefficients $\binom{n}{k}$ for $k = 0 \ldots n$

$$\begin{array}{lccccccccccc}
n=0: & & & & & & 1 & & & & & \\
n=1: & & & & & 1 & & 1 & & & & \\
n=2: & & & & 1 & & 2 & & 1 & & & \\
n=3: & & & 1 & & 3 & & 3 & & 1 & & \\
n=4: & & 1 & & 4 & & 6 & & 4 & & 1 & \\
n=5: & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
\vdots & & & & & & \vdots & & & & &
\end{array}$$

* each number is the sum of the two above it

Note:

$$\binom{m+1}{n+1} = \binom{m}{n} + \binom{m}{n+1}$$

Proof. We want to choose $n+1$ elements from the set $\{1, 2, \ldots m+1\}$. Either $m+1$ is one of the $n+1$ chosen elements or it is not. If it is, task is to choose n from m, which is the first term. If it isn't, task is to choose $n+1$ from m, which is the second term. $\blacksquare$

Number Theoretic Properties

Factorials - let p be a prime and n be a natural number. Question is "what power of p exactly divides $n!$?"

Notation: For real number x, then $\lfloor x \rfloor$ is the highest integer $\leq x$

Claim

$$p^e || n!, \quad e = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor \dots$$

$||$ means exactly divides $\Rightarrow p^e | n!,\ p^{e+1} \nmid n!$

Proof. $n! = n(n-1)\dots 1$
$\left\lfloor \frac{n}{p} \right\rfloor$ = number of multiples of p in $\{1, 2, \dots n\}$
$\left\lfloor \frac{n}{p^2} \right\rfloor$ = number of multiples of p^2 in $\{1, 2, \dots n\}$, etc. ∎

Note: There is an easy bound on e:

$$\begin{aligned} e &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor \dots \\ &\leq \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} \dots \\ &\leq \frac{\frac{n}{p}}{1 - \frac{1}{p}} \\ &\leq \frac{n}{p-1} \end{aligned}$$

Proposition 13. *Write n in base p, so that $n = a_0 + a_1 p + a_2 p^2 \dots a_k p^k$, with $a_i \in \{0, 1 \dots p-1\}$. Then*

$$e(a,p) = \frac{n - (a_0 + a_1 \dots + a_k)}{p-1}$$

Proof. With the above notation, we have

$$\begin{aligned}
\left\lfloor \frac{n}{p} \right\rfloor &= a_1 + a_2 p \dots a_k p^{k-1} \\
\left\lfloor \frac{n}{p^2} \right\rfloor &= a_2 + a_3 p \dots a_k p^{k-1}, \text{ etc.} \\
&\vdots \\
a_0 &= n - p \left\lfloor \frac{n}{p} \right\rfloor \\
a_1 &= \qquad \left\lfloor \frac{n}{p} \right\rfloor - p \left\lfloor \frac{n}{p^2} \right\rfloor, \text{ etc.} \\
&\vdots \\
\sum_{i=0}^{k} a &= n - (p-1)\left(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor \dots \right) \\
\sum_{i=0}^{k} a &= n - (p-1)(e) \\
e &= \frac{n - \sum_{i=0}^{k} a}{p-1}
\end{aligned}$$

■

Corollary 14. *The power of prime p dividing $\binom{n}{k}$ is the number of carries when you add k to $n-k$ in base p (and also the number of carries when you subtract k from n in base p)*

Some nice consequences:

- Entire $(2^k - 1)^{\text{th}}$ row of Pascal's Triangle consists of odd numbers
- 2^nth row of triangle is even, except for 1s at the end
- $\binom{p}{k}$ is divisible by prime p for $0 < k < p$ (p divides numerator and not denominator)
- $\binom{p^e}{k}$ is divisible by prime p for $0 < k < p^e$

(Definition) Congruence: Let a, b, m be integers, with $m \neq 0$. We say a is **congruent** to b modulo m ($a \equiv b \mod m$) if $m|(a-b)$ (ie., a and b have the same remainder when divided by m

Congruence compatible with usual arithmetic operations of addition and multiplication.

ie., if $a \equiv b \mod m$ and $c \equiv d \mod m$

$$a + c \equiv b + d \pmod{m}$$
$$ac \equiv bd \pmod{m}$$

Proof.

$$\begin{aligned} a &= b + mk \\ c &= d + ml \\ a + c &= b + d + m(k + l) \\ ac &= bd + bml + dmk + m^2kl \\ &= bd + m(bl + dk + mkl) \end{aligned}$$

■

* This means that if $a \equiv b \mod m$, then $a^k \equiv b^k \mod m$, which means that if $f(x)$ is some polynomial with integer coefficients, then $f(a) \equiv f(b) \mod m$

NOT TRUE: if $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a^c \equiv b^d \mod m$

NOT TRUE: if $ax \equiv bx \mod m$, then $a \equiv b \mod m$ (essentially because $(x, m) > 1$). But if $(x, m) = 1$, then true.

Proof. $m|(ax - bx) = (a - b)x$, m coprime to x means that $m|(a - b)$ ■

Lecture 4
FFermat, Euler, Wilson, Linear Congruences

(Definition) Complete Residue System: A **complete residue system mod** m is a collection of integers $a_1 \dots a_m$ such that $a_i \not\equiv a_j \mod m$ if $i \neq j$ and any integer n is congruent to some $a_i \mod m$

(Definition) Reduced Residue System: A **reduced residue system mod** m is a collection of integers $a_1 \dots a_k$ such that $a_i \not\equiv a_j \mod m$ if $i \neq j$ and $(a_i, m) = 1$ for all i, and any integer n coprime to m must be congruent to some $a_i \mod m$. Eg., take any complete residue system mod m and take the subset consisting of all the integers in it which are coprime to m - these will form a reduced residue system

Eg. For $m = 12$
complete = $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
reduced = $\{1, 5, 7, 11\}$

(Definition) Euler's Totient Function: The number of elements in a reduced residue system mod m is called **Euler's totient function**: $\phi(m)$ (ie., the number of positive integers $\leq m$ and coprime to m)

Theorem 15 (Euler's Theorem)**.**

$$\textit{If } (a, m) = 1, \textit{ then } a^{\phi(m)} \equiv 1 \mod m$$

Proof.

Lemma 16. *If $(a, m) = 1$ and $r_1 \dots r_k$ is a reduced residue system mod m, $k = \phi(m)$, then $ar_1 \dots ar_k$ is also a reduced residue system mod m.*

Proof. All we need to show is that ar_i are all coprime to m and distinct mod m, since there are k of these ar_i and k is the number of elements in any residue system mod m. We know that if $(r, m) = 1$ and $(a, m) = 1$ then $(ar, m) = 1$. Also, if we had $ar_i \equiv ar_j \mod m$, then $m | ar_i - ar_j = a(r_i - r_j)$. If $(a, m) = 1$ then $m | r_i - r_j \Rightarrow r_i \equiv r_j \mod m$, which cannot happen unless $i = j$. $\square$

Choose a reduced residue system $r_1 \dots r_k \mod m$ with $k = \phi(m)$. By lemma, $ar_1 \dots ar_k$ is also a reduced residue system. These two must be permutations of each other mod m (ie., $ar_i \equiv r_{j(i)} \mod m$).

$$\begin{aligned} r_1 r_2 \dots r_k &\equiv ar_1 ar_2 \dots ar_k \pmod m \\ r_1 r_2 \dots r_k &\equiv a^{\phi(m)} r_1 r_2 \dots r_k \pmod m \\ (r_1 r_2 \dots r_k, m) = 1 &\Rightarrow \text{ can cancel} \\ a^{\phi(m)} &\equiv 1 \pmod m \end{aligned}$$

■

Corollary 17 (Fermat's Little Theorem)**.**

$$a^p \equiv a \pmod p \quad \textit{for prime } p \textit{ and integer } a$$

Proof. If $p \nmid a$ (ie., $(a,p) = 1$) then $a^{\phi(p)} \equiv 1 \mod p$ by Euler's Theorem. $\phi(p) = p - 1 \Rightarrow a^{p-1} \equiv 1 \mod p \Rightarrow a^p \equiv a \mod p$. If $p|a$, then $a \equiv 0 \mod p$ so both sides are $0 \equiv 0 \mod p$. ■

Proof by induction.

Lemma 18 (Freshman's Dream)**.**

$$(x+y)^p \equiv x^p + y^p \pmod p \quad x, y \in \mathbb{Z}, \textit{ prime } p$$

Use the Binomial Theorem.

$$(x+y)^p = x^p + y^p + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}}_{\equiv 0 \mod p}$$

We saw that $\binom{p}{k}$ is divisible by p for $1 \leq k \leq p-1$, so

$$(x+y)^p \equiv x^p + y^p \pmod p$$

□

Induction base case of $a = 0$ is obvious. Check to see if it holds for $a+1$ assuming it holds for a

$$\begin{aligned} (a+1)^p - (a+1) &\equiv a^p + 1 - (a+1) \pmod p \\ &\equiv a^p - a \pmod p \\ &\equiv 0 \pmod p \\ (a+1)^p &\equiv (a+1) \pmod p \end{aligned}$$

This is reversible (if holds for a, then also for $a-1$), and so holds for all integers by stepping up or down ■

Proposition 19 (Inverses of elements mod m). *If $(a, m) = 1$, then there is a unique integer $b \mod m$ such that $ab \equiv 1 \mod m$. This b is denoted by $\frac{1}{a}$ or $a^{-1} \mod m$*

Proof of Existence. Since $(a, m) = 1$ we know that $ax + my = 1$ for some integers x, y, and so $ax \equiv 1 \mod m$. Set $b = x$. ■

Proof of Uniqueness. If $ab_1 \equiv 1 \mod m$ and $ab_2 \equiv 1 \mod m$, then $ab_1 \equiv ab_2 \mod m \Rightarrow m|a(b_1 - b_2)$. Since $(m, a) = 1$, $m|b_1 - b_2 \Rightarrow b_1 \equiv b_2 \mod m$. ■

Theorem 20 (Wilson's Theorem). *If p is a prime then $(p-1)! \equiv -1 \mod p$*

Proof. Assume that p is odd (trivial for $p = 2$).

Lemma 21. *The congruence $x^2 \equiv 1 \mod p$ has only the solutions $x \equiv \pm 1 \mod p$*

Proof.

$$\begin{aligned} & x^2 \equiv 1 \mod p \\ \Rightarrow\ & p | x^2 - 1 \\ \Rightarrow\ & p | (x-1)(x+1) \\ \Rightarrow\ & p | x \pm 1 \\ \Rightarrow\ & x \equiv \pm 1 \mod p \end{aligned}$$

□

Note that $x^2 \equiv 1 \mod p \Rightarrow (x, p) = 1$ and x has inverse and $x \equiv x^{-1} \mod p$ $\{1 \ldots p-1\}$ is a reduced residue system mod p. Pair up elements a with inverse $a^{-1} \mod p$. Only singletons will be 1 and -1.

$$\begin{aligned} (p-1)! &\equiv (a_1 \cdot a_1^{-1})(a_2 \cdot a_2^{-1}) \ldots (a_k \cdot a_k^{-1})(1)(-1) \pmod p \\ &\equiv -1 \pmod p \end{aligned}$$

■

Wilson's Theorem lets us solve congruence $x^2 \equiv -1 \mod p$

Theorem 22. *The congruence $x^2 \equiv -1 \mod p$ is solvable if and only if $p = 2$ or $p \equiv 1 \mod 4$*

Proof. $p = 2$ is easy. We'll show that there is no solution for $p \equiv 3 \mod 4$ by contradiction. Assume $x^2 \equiv -1 \mod p$ for some x coprime to p ($p = 4k + 3$). Note that

$$p - 1 = 4k + 2 = 2(2k + 1)$$

so $(x^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \mod p$. But also,

$$(x^2)^{2k+1} \equiv x^{4k+2} \equiv x^{p-1} \equiv 1 \mod p$$

So $1 \equiv -1 \mod p \Rightarrow p|2$, which is impossible since p is an odd prime.

If $p \equiv 1 \mod 4$:

$$\begin{aligned}
(p-1)! &\equiv -1 \pmod p \text{ by Wilson's Theorem} \\
(1)(2)\dots(p-1) &\equiv -1 \pmod p \\
\underbrace{\left(1 \cdot 2 \dots \frac{p-1}{2}\right)}_{x} \underbrace{\left(\frac{p+1}{2} \dots p-1\right)}_{\substack{\text{show that second factor} \\ \text{equals the first}}} &\equiv -1 \pmod p
\end{aligned}$$

$$\begin{aligned}
p - 1 &\equiv (-1)1 \pmod p \\
p - 2 &\equiv (-1)2 \pmod p \\
&\vdots \\
\frac{p+1}{2} &\equiv (-1)\frac{p-1}{2} \pmod p \\
\underbrace{\left(\frac{p+1}{2}\right)\dots(p-1)}_{\text{second factor}} &\equiv (-1)^{\frac{p-1}{2}} \underbrace{\left(1 \cdot 2 \dots \left(\frac{p-1}{2}\right)\right)}_{x} \pmod p
\end{aligned}$$

$\frac{p-1}{2}$ is even since $p \equiv 1 \mod 4$, and so second factor equals the first factor, so $x = \left(\frac{p-1}{2}\right)!$ solves $x^2 \equiv -1 \mod p$ if $p \equiv 1 \mod 4$. ■

Theorem 23. *There are infinitely many primes of form* $4k + 1$

Proof. As in Euclid's proof, assume finitely many such primes $p_1 \dots p_n$. Consider the positive integer

$$N = (2p_1p_2 \dots p_n)^2 + 1$$

N is an odd integer > 1, so it has an odd prime factor $q \neq p_i$, since each p_i divides $N - 1$. $q|N \Rightarrow (2p_1 \dots p_n)^2 \equiv -1 \mod q$, so $x^2 \equiv -1 \mod q$ has a solution and so by theorem $q \equiv 1 \mod 4$, which contradicts $q \neq p_i$. ■

(Definition) Congruence: A **congruence** (equation) is of the form $a_n x^n + a_{n-1}x^{n-1} \cdots + a_0 \equiv 0 \mod m$ where $a_n \ldots a_0$ are integers. Solution of the congruence are integers or residue classes mod m that satisfy the equation.

Eg. $x^p - x \equiv 0 \mod p$. How many solutions? p.

Eg. $x^2 \equiv -1 \mod 5$. Answers $= 2, 3$.

Eg. $x^2 \equiv -1 \mod 43$. No solutions since $43 \equiv 3 \mod 4$.

Eg. $x^2 \equiv 1 \mod 15$. Answers $= \pm 1, \pm 4 \mod 15$.

Note: The number of solutions to a non-prime modulus can be larger than the degree

(Definition) Linear Congruence: a congruence of degree 1 ($ax \equiv b \mod m$)

Theorem 24. *Let $g = (a, m)$. Then there is a solution to $ax \equiv b \mod m$ if and only if $g|b$. If it has solutions, then it has exactly g solutions mod m.*

Proof. Suppose $g \nmid b$. We want to show that the congruence doesn't have a solution. Suppose x_0 is a solution $\Rightarrow ax_0 = b + mk$ for some integer k. Since $g|a,\ g|m$, g divides $ax_0 - mk = b$, which is a contradiction. Conversely, if $g|b$, we want to show that solutions exist. We know $g = ax_0 + my_0$ for integer x_0, y_0. If $b = b'g$, multiply by b' to get

$$\begin{aligned} b = b'g &= b'|ax_0 + my_0 \\ &= a(b'x_0) + m(b'y_0) \\ &\Rightarrow a(b'x_0) \equiv b \pmod m \end{aligned}$$

and so $x = b'x_0$ is a solution.

We need to show that there are exactly g solutions. We know that there is one solution x_1, and the congruence says $ax \equiv b \equiv ax_1 \mod m$.

$$\begin{aligned} a(x - x_1) &\equiv 0 \pmod m \\ a(x - x_1) &\equiv mk \text{ for some integer } k \\ g = (a, m) &\Rightarrow a = a'g,\ m = m'g \end{aligned}$$

So $(a, m') = 1$, so $a'g(x - x_1) = m'gk \Rightarrow a(x - x_1) = m'k$ for some k. So $m'|x - x_1$, so $x \equiv x_1 \mod m'$, so any solution of the congruence must be congruent to x

$\bmod m' = m$. So all the solutions are $x_1, x_1 + m', x_1 + 2m', \ldots, x_1 + (g-1)m'$. They are all distinct, so they are all the solutions mod m. ■

03/19/2015 Number Theory

Chpt2. Congruences

True Or False

1) If $a \equiv b \bmod m$, $c \equiv d \bmod m$. then $a^c \equiv b^d \bmod m$

$\boxed{\text{False}}$ $2 \equiv 2 \pmod 3$ $1 \equiv 4 \bmod 3$

But $2^1 \equiv 2\ (3)$ $2^4 \equiv 1\ (3)$

2) If $a \equiv b\ (m)$ $c \equiv d\ (m)$, then $ac \equiv bd\ (m)$ True

3) If $ax \equiv bx\ (m)$, then $a \equiv b\ (m)$ False

eg $x = 2$, $m = 2$

what if $(x, m) = 1$? True

Basic Properties Theorem 2.1, 2.2 a, b, c, d — integers, then

1) If $a \equiv b\ (m)$, $b \equiv a\ (m)$ & $a - b \equiv 0\ (m)$ are equivalent

2) If $a \equiv b\ (m)$ $b \equiv c\ (m)$, then $a \equiv c\ (m)$

3) If $a \equiv b\ (m)$, $c \equiv d\ (m)$. $a \pm c \equiv b \pm d\ (m)$, $ac \equiv bd\ (m)$

4) ~~If $a \equiv b\ (m)$, $c \equiv d\ (m)$, $d \mid m$, then~~ a

4): If $a \equiv b (m)$, $d | m$ & $d > 0$, then $a \equiv b \ (d)$

5): If $a \equiv b \ (m)$, then $ac \equiv bc \ (mc)$ for $c > 0$

6): Let $f \in \mathbb{Z}[x]$ — polynomial with integer coefficients. If $a \equiv b \ (m)$ then $f(a) \equiv f(b) \ (m)$

Thm. 2.3.

(I): $ax \equiv ay \ (\text{mod } m)$ iff $x \equiv y \ (\text{mod } \frac{m}{(a,m)})$

(II): If $ax \equiv ay \ (m)$ and $(a,m) = 1$, then $x \equiv y \ (m)$

(III): $x \equiv y \ (m_i)$ for $i = 1, 2, \cdots, r$. iff $x \equiv y \ (\text{mod } [m_1, \cdots, m_r])$

[proof]: (I) $ax \equiv ay \Leftrightarrow ax - ay = m \cdot N \Leftrightarrow \frac{ax - ay}{(m,a)} = \frac{m}{(m,a)} N$

$\Leftrightarrow \frac{a}{(m,a)} (x-y) = \frac{m}{(m,a)} N$

$\rightarrow \frac{m}{(m,a)} \Big| (x-y) \Rightarrow x \equiv y \ (\frac{m}{(m,a)})$

$\Leftarrow$ if $x \equiv y \ (\frac{m}{(m,a)}) \Rightarrow a(x-y) = a(N \cdot \frac{m}{(m,a)})$ ✓.

II (last time)

III: If $x \equiv y \ (m_i)$. then $m_i \,|\, y - x$ for all i;

$\Rightarrow [m_1, \cdots, m_r] \,|\, x - y$; If $[m_1, \cdots, m_r] \,|\, x - y \Rightarrow$ ✓

Recall: A complete residue system mod (m) is a set of integers $x_1, \dots, x_m$ s.t. for every integer y there exists a unique x_j in the set s.t. $y \equiv x_j \ (m)$

$\boxed{eg}$ $m = 3$.

complete residue system: $\{-2, -1, 0\}$

$\{-2, 2, 0\}$, $\{30, 29, 28\}$, — —

NOT $\{1, 3, 4\}$ as $1 \equiv 4 \ (3)$

The set is call a residue class or congruence clas. mod m. ~~There are always~~

Thm: If $b \equiv c \ (m)$ then $(b, m) = (c, m)$

idea: $b = mx + c$ (the proof for finding GCD)

Recall: A reduced Residue System mod m.

1) $\{a_1, \dots, a_k\}$ s.t. $a_i \not\equiv a_j \ (m) \ \forall \ i \neq j$.

2) ~~[illegible]~~ $(a_i, m) = 1$ for all i

3) any int. n coprime to m is congruent to some a_i

02/19/2015 Number Theory

Chapter 2. Congruences

Lecture 7
FFermat, Euler, Wilson, Linear Congruences

(Definition) Complete Residue System: A complete residue system mod m is a collection of integers $a_1 \dots a_m$ such that $a_i \not\equiv a_j \mod m$ if $i \neq j$ and any integer n is congruent to some $a_i \mod m$

(Definition) Reduced Residue System: A reduced residue system mod m is a collection of integers $a_1 \dots a_k$ such that $a_i \not\equiv a_j \mod m$ if $i \neq j$ and $(a_i, m) = 1$ for all i, and any integer n coprime to m must be congruent to some $a_i \mod m$. Eg., take any complete residue system mod m and take the subset consisting of all the integers in it which are coprime to m - these will form a reduced residue system

Eg. For $m = 12$
complete $= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
reduced $= \{1, 5, 7, 11\}$

For prime numbers complete/p are reduced

(Definition) Euler's Totient Function: The number of elements in a reduced residue system mod m is called **Euler's totient function:** $\phi(m)$ (ie., the number of positive integers $\leq m$ and coprime to m)

<

Theorem 15 (Euler's Theorem).

$$\textit{If } (a, m) = 1, \textit{ then } a^{\phi(m)} \equiv 1 \mod m$$

☆

Proof.

Lemma 16. *If $(a, m) = 1$ and $r_1 \dots r_k$ is a reduced residue system mod m, $k = \phi(m)$, then $ar_1 \dots ar_k$ is also a reduced residue system mod m.*

Proof. All we need to show is that ar_i are all coprime to m and distinct mod m, since there are k of these ar_i and k is the number of elements in any residue system mod m. We know that if $(r, m) = 1$ and $(a, m) = 1$ then $(ar, m) = 1$. Also, if we had $ar_i \equiv ar_j \mod m$, then $m | ar_i - ar_j = a(r_i - r_j)$. If $(a, m) = 1$ then $m | r_i - r_j \Rightarrow r_i \equiv r_j \mod m$, which cannot happen unless $i = j$. ☐

Choose a reduced residue system $r_1 \dots r_k \mod m$ with $k = \phi(m)$. By lemma, $ar_1 \dots ar_k$ is also a reduced residue system. These two must be permutations of each other mod m (ie., $ar_i \equiv r_{j(i)} \mod m$).

$$\begin{aligned} r_1 r_2 \dots r_k &\equiv ar_1 ar_2 \dots ar_k \pmod{m} \\ r_1 r_2 \dots r_k &\equiv a^{\phi(m)} r_1 r_2 \dots r_k \pmod{m} \\ (r_1 r_2 \dots r_k, m) = 1 &\Rightarrow \text{ can cancel} \\ a^{\phi(m)} &\equiv 1 \pmod{m} \end{aligned}$$

■

Corollary 17 (Fermat's Little Theorem).

$$a^p \equiv a \pmod{p} \quad \textit{for prime } p \textit{ and integer } a$$

Proof. If $p \nmid a$ (ie., $(a,p) = 1$) then $a^{\phi(p)} \equiv 1 \mod p$ by Euler's Theorem. $\phi(p) = p - 1 \Rightarrow a^{p-1} \equiv 1 \mod p \Rightarrow a^p \equiv a \mod p$. If $p \mid a$, then $a \equiv 0 \mod p$ so both sides are $0 \equiv 0 \mod p$. ■

Proof by induction.

Lemma 18 (Freshman's Dream).

$$(x+y)^p \equiv x^p + y^p \pmod{p} \quad x, y \in \mathbb{Z}, \textit{ prime } p$$

Use the Binomial Theorem.

$$(x+y)^p = x^p + y^p + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}}_{\equiv 0 \mod p}$$

We saw that $\binom{p}{k}$ is divisible by p for $1 \leq k \leq p-1$, so

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

□

Induction base case of $a = 0$ is obvious. Check to see if it holds for $a+1$ assuming it holds for a

$$\begin{aligned} (a+1)^p - (a+1) &\equiv a^p + 1 - (a+1) \pmod{p} \\ &\equiv a^p - a \pmod{p} \\ &\equiv 0 \pmod{p} \\ (a+1)^p &\equiv (a+1) \pmod{p} \end{aligned}$$

This is reversible (if holds for a, then also for $a-1$), and so holds for all integers by stepping up or down ■

Proposition 19 (Inverses of elements mod m). *If $(a,m)=1$, then there is a unique integer $b \mod m$ such that $ab \equiv 1 \mod m$. This b is denoted by $\frac{1}{a}$ or $a^{-1} \mod m$*

Proof of Existence. Since $(a,m)=1$ we know that $ax+my=1$ for some integers x,y, and so $ax \equiv 1 \mod m$. Set $b=x$. ■

Proof of Uniqueness. If $ab_1 \equiv 1 \mod m$ and $ab_2 \equiv 1 \mod m$, then $ab_1 \equiv ab_2 \mod m \Rightarrow m|a(b_1-b_2)$. Since $(m,a)=1$, $m|b_1-b_2 \Rightarrow b_1 \equiv b_2 \mod m$. ■

Theorem 20 (Wilson's Theorem). *If p is a prime then $(p-1)! \equiv -1 \mod p$*

Proof. Assume that p is odd (trivial for $p=2$).

Lemma 21. *The congruence $x^2 \equiv 1 \mod p$ has only the solutions $x \equiv \pm 1 \mod p$*

Proof.

$$\begin{aligned} & x^2 \equiv 1 \mod p \\ & \Rightarrow p|x^2-1 \\ & \Rightarrow p|(x-1)(x+1) \\ & \Rightarrow p|x \pm 1 \\ & \Rightarrow x \equiv \pm 1 \mod p \end{aligned}$$

□

Note that $x^2 \equiv 1 \mod p \Rightarrow (x,p)=1$ and x has inverse and $x \equiv x^{-1} \mod p$
$\{1 \dots p-1\}$ is a reduced residue system mod p. Pair up elements a with inverse $a^{-1} \mod p$. Only singletons will be 1 and -1.

1's inverse is 1, (-1)'s inverse is (-1)

$$\begin{aligned} (p-1)! &\equiv (a_1 \cdot a_1^{-1})(a_2 \cdot a_2^{-1}) \dots (a_k \cdot a_k^{-1})(1)(-1) \pmod p \\ &\equiv -1 \pmod p \end{aligned}$$

■

Wilson's Theorem lets us solve congruence $x^2 \equiv -1 \mod p$

Theorem 22. *The congruence $x^2 \equiv -1 \mod p$ is solvable if and only if $p=2$ or $p \equiv 1 \mod 4$*

Proof. $p = 2$ is easy. We'll show that there is no solution for $p \equiv 3 \mod 4$ by contradiction. Assume $x^2 \equiv -1 \mod p$ for some x coprime to p ($p = 4k+3$). Note that

$$p - 1 = 4k + 2 = 2(2k+1)$$

so $(x^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \mod p$. But also,

$$(x^2)^{2k+1} \equiv x^{4k+2} \equiv x^{p-1} \equiv 1 \mod p$$

So $1 \equiv -1 \mod p \rightarrow p|2$, which is impossible since p is an odd prime.

If $p \equiv 1 \mod 4$:

$$\begin{aligned}
(p-1)! &\equiv -1 \pmod p \text{ by Wilson's Theorem} \\
(1)(2)\dots(p-1) &\equiv -1 \pmod p \\
\underbrace{\left(1 \cdot 2 \dots \frac{p-1}{2}\right)}_{x} \underbrace{\left(\frac{p-1}{2} \dots p-1\right)}_{\substack{\text{show that second factor} \\ \text{equals the first}}} &\equiv -1 \pmod p
\end{aligned}$$

$$\begin{aligned}
p - 1 &\equiv (-1)1 \pmod p \\
p - 2 &\equiv (-1)2 \pmod p \\
&\vdots \\
\frac{p+1}{2} &\equiv (-1)\frac{p-1}{2} \pmod p \\
\underbrace{\left(\frac{p+1}{2}\right) \dots (p-1)}_{\text{second factor}} &\equiv (-1)^{\frac{p-1}{2}} \underbrace{\left(1 \cdot 2 \dots \left(\frac{p-1}{2}\right)\right)}_{x} \pmod p
\end{aligned}$$

$\frac{p-1}{2}$ is even since $p \equiv 1 \mod 4$, and so second factor equals the first factor, so $x = \left(\frac{p-1}{2}\right)!$ solves $x^2 \equiv -1 \mod p$ if $p \equiv 1 \mod 4$. ■

Theorem 23. *There are infinitely many primes of form* $4k+1$

Proof. As in Euclid's proof, assume finitely many such primes $p_1 \dots p_n$. Consider the positive integer

$$N = (2p_1p_2 \dots p_n)^2 + 1$$

N is an odd integer > 1, so it has an odd prime factor $q \neq p_i$, since each p_i divides $N - 1$. $q|N \Rightarrow (2p_1 \dots p_n)^2 \equiv -1 \mod q$, so $x^2 \equiv -1 \mod q$ has a solution and so by theorem $q \equiv 1 \mod 4$, which contradicts $q \neq p_i$. ■

02/24/2015 / Number Theory

Recall:

1) Euler's Theorem. If $(a,m)=1$, then $a^{\phi(m)} \equiv 1 \mod m$

Two meanings: ~~X~~ if $(a,m)=1$, then a is invertible mod m & $a^{-1} \equiv a^{\phi(m)-1} \pmod m$

$\phi(m) :=$ size of Reduced Residue system (mod m)

$=$ size of $\{a \mid 0<a<m,\ (a,m)=1\}$

eg: $\phi(10) = ?$

Find #'s rel. prime to 10 & < 10

$1, 3, 7, 9 \implies \phi(10)=4$

& by Euler's Theorem: $1^4 \equiv 1\ (10)$, $3^4 \equiv 1\ (10)$

$7^4 \equiv 1\ (10)$, $9^4 \equiv 1\ (10)$

Thm from last Time: Inverse of 1 (mod 10) is 1

Inverse of 9 (mod 10) (i.e. -1 mod 10) is -1

Inverse of $7 \pmod{10}$.

Two ways to find out ① $7 \cdot 7^3 \equiv 1 \ (10)$

$\Rightarrow 7^3 \pmod{10}$ is 7^{-1}

$\equiv 343 \pmod{10}$

$\equiv 3 \pmod{10}$

$\Rightarrow 7^{-1} \equiv 3 \ (10)$ & $3^{-1} \equiv 7 \ (10)$

②: since $(7,10)=1$. we can find a, b

s.t. $7a + 10b = 1$ use Euclidean Algorithm

		10	7
①	10	1	0
②	7	0	1
~~2×~~①-②	3	1	-1
	$1=7-2\cdot 3$	-2	3

$10 \cdot (-2) + 7 \cdot 3 = 1$

$\Rightarrow 10(-2) + 7 \cdot 3 \equiv 1 \ (10)$

$7 \cdot 3 \equiv 1 \ (10)$

$7^{-1} \equiv 3 \ (10)$

2) <u>Fermat's Little Theorem</u>: $a^p \equiv a \ (p)$ if p is a prime

3) Solution to $x^2 \equiv 1 \ (p)$: $x \equiv \pm 1 \ (p)$

4) $x^2 \equiv -1 \ (p)$ is solvable $\Leftrightarrow$ $p = 2$ or $p \equiv 1 \ (4)$

(Definition) Congruence: A congruence (equation) is of the form $a_n x^n + a_{n-1}x^{n-1} \cdots + a_0 \equiv 0 \mod m$ where $a_n \ldots a_0$ are integers. Solution of the congruence are integers or residue classes mod m that satisfy the equation.

p=prime Eg. $x^p - x \equiv 0 \mod p$. How many solutions? p. (Fermat's little theorem)

Eg. $x^2 \equiv -1 \mod 5$. Answers $= 2, 3$.

Eg. $x^2 \equiv -1 \mod 43$. No solutions since $43 \equiv 3 \mod 4$.

Eg. $x^2 \equiv 1 \mod 15$. Answers $= \pm 1, \pm 4 \mod 15$.

Note: The number of solutions to a non-prime modulus can be larger than the degree (not true over $\mathbb{R}, \mathbb{C}, \ldots$)

(Definition) Linear Congruence: a congruence of degree 1 ($ax \equiv b \mod m$)

Theorem 24. *Let $g = (a, m)$. Then there is a solution to $ax \equiv b \mod m$ if and only if $g|b$. If it has solutions, then it has exactly g solutions mod m.*

existence

Proof. Suppose $g \nmid b$. We want to show that the congruence doesn't have a solution. Suppose x_0 is a solution $\Rightarrow ax_0 = b + mk$ for some integer k. Since $g|a$, $g|m$, g divides $ax_0 - mk = b$, which is a contradiction. Conversely, if $g|b$, we want to show that solutions exist. We know $g = ax_0 + my_0$ for integer x_0, y_0. If $b = b'g$, multiply by b' to get

$$\begin{aligned} b = b'g &= b'(ax_0 + my_0) \\ &= a(b'x_0) + m(b'y_0) \\ &\Rightarrow a(b'x_0) \equiv b \pmod m \end{aligned}$$

and so $x = b'x_0$ is a solution. (this provide a way of finding solutions)

g solutions

We need to show that there are exactly g solutions. We know that there is one solution x_1, and the congruence says $ax \equiv b \equiv ax_1 \mod m$.

$$\begin{aligned} &a(x - x_1) \equiv 0 \pmod m \\ &a(x - x_1) = mk \text{ for some integer } k \\ &g = (a, m) \Rightarrow a = a'g,\ m = m'g \end{aligned}$$

So $(a, m') = 1$, so $a'g(x - x_1) = m'gk \Rightarrow a'(x - x_1) = m'k$ for some k. So $m'|x - x_1$, so $x \equiv x_1 \mod m'$, so any solution of the congruence must be congruent to x

mod $m' \mid m$. So all the solutions are $x_1, x_1 + m', x_1 + 2m', \ldots, x_1 + (g-1)m'$. They are all distinct, so they are all the solutions mod m. ■

(later)

$\boxed{\text{eg}}$. Determine if the following congruences have solutions if so, find all of them.

1) $15x \equiv 36 \ (17)$

2) $4x \equiv 8 \ (16)$

3) $6x \equiv 14 \ (12)$

4) $4x \equiv 2 \ (14)$

~~Lecture 5~~ Section 2.2 Solution of Congruences.

Linear Congruences, Chinese Remainder Theorem, Algorithms

Recap - linear congruence $ax \equiv b \mod m$ has solution if and only if $g = (a, m)$ divides b. How do we find these solutions?

Case 1: $g = (a, m) = 1$. Then invert $a \mod m$ to get $x \equiv a^{-1}b \mod m$. Algorithmically, find $ax_0 + my_0 = 1$ with Euclidean Algorithm, then $ax_0 \equiv 1 \mod m$ so $x_0 = a^{-1}$, so $x \equiv x_0 b = a^{-1}b$ solves the congruence. ($ax \equiv a(x_0 b) \equiv (ax_0)b \equiv b \mod m$). Conclusion: There is a unique solution mod m.

Case 2: $g = (a, m) > 1$. If $g \nmid b$, there are no solutions. If $g | b$, write $a = a'g, b = b'g, m = m'g$ so that $ax \equiv b \mod m \Rightarrow a'x = b' \mod m'$ so that (a', m') is now 1. The unique solution (found by Case 1) $x \mod m'$ also satisfied $ax \equiv b \mod m$ so that we have one solution mod m. We know any solution $\tilde{x} \mod m$ must be congruent to $x \mod m'$, so $\tilde{x}$ must have form $x + m'k$ for some k. As k goes from 0 through $g - 1$ we get the g distinct integers mod m: $x, x + m', x + 2m' \ldots x + (g-1)m'$, which all satisfy $a\tilde{x} \equiv b \mod m$ because

$$\begin{aligned} a(x + km') &= ax + akm' \\ &= ax + a'gkm' \\ &= ax + m(a'k) \\ &\equiv ax \pmod m \\ &\equiv b \pmod m \end{aligned}$$

Conclusion: this congruence has $g = (a, m)$ solutions mod m.

Eg.,

$$35x \equiv 14 \pmod{28}$$

$(35, 28) = g = 7$. To solve, first divide through by 7 to get $5x \equiv 2 \mod 4$. Solution of $x \equiv 2 \mod 4$ is $x = 2$, which will also satisfy original congruence. $m' = \frac{28}{7} = 4 \Rightarrow$ all solutions mod $28 \equiv 2, 6, 10, 14, 18, 22, 26$.

Note $(5, 2) = 1$

	5	2
5	1	0
2	0	1
1	1	-2

$5 + (-2)\cdot 2 = 1$

Note $5^{-1} = 1$

Simultaneous System of Congruences to Different Moduli: Given

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

Does this system have a common solution? (Not always, eg., $x \equiv 3 \mod 8$ and $x \equiv 1 \mod 12$) In general, need some compatibility conditions.

$\boxed{eg}$:

$10x \equiv 5 \ (6)$

$(10, 6) = 2$

But $2 \nmid 5$

No solution

$\boxed{eg}$:

$10x \equiv 14 \ (6)$

$\boxed{\text{make it easy}}$

$4x \equiv 2 \ (6)$

$(4, 6) = 2$, $2 | 2$

$\Rightarrow 2x \equiv 1 \ (3)$

$2^{-1} \equiv 2 \ (3)$

$x \equiv 2 (3)$

Note 2 solutions modula 3

$2, 2 + \frac{6}{2}$

test $2 \cdot 10 = 20$

$20 (6) \equiv 2$ ✓

$(2 + \frac{6}{2}) \cdot 10 = 50$

$50 (6) \equiv 2$ ✓

1). $15x \equiv 36 \ (17)$

simplify : $15x \equiv 2 \ (17)$, $(15,17)=1$, $(2,17)=1$

Find $15^{-1} \ (17)$ either $15^{\varphi(17)-1} \equiv 15^{-1} \ (17)$

Hard!

or GCD

		17	15
	17	1	0
	15	0	1
-7	2	1	-1
	1	-7	8

$$17(-7) + 15\cdot(8) = 1$$

so $15^{-1} \equiv 8 \ (17)$.

$\Rightarrow x \equiv 2\cdot 8 \ (17)$

$\equiv 16$

unique solution as $(15,17)=1$

$ax \equiv b \ (m)$

2). $4x \equiv 8 \ (16)$, $(4,16)=4$, & $4 \mid 8$

# of solutions $= (4,16) = 4$

Find 1 solution | First Solve: $g = a x_0 + m y_0$

Method ①

1.e. Solve: $4 = 4x_0 + 16y_0$ (easy: by observation) $x_0 = (-3)$, $y_0 = 1$ 8

$$b \equiv b'g \equiv b'(ax_0 + my_0) \equiv b'ax_0 \quad (m)$$
$$\equiv a(b'x_0) \ (m)$$

or solve: $\frac{a}{g}x \equiv \frac{b}{g} \left(\frac{m}{g}\right)$

$b' = b/g = 8/4 = 2 \Rightarrow$ ONE Solution $b'x_0 \equiv 2 \cdot (-3) \ (16)$

Totally $\overset{=4}{g}$ Solutions (mod 16): -6, $-6 + \frac{m}{g} = \frac{16}{4} = 4$

$\underline{-6}$, $\underline{-2}$, $\underline{-2+4=2}$, $\underline{2+4=6}$

plug solutions back in to see if they are correct.

3): $6x \equiv 14 \ (12)$ $(6,12) = 6$, $6 \nmid 14$ No solu.

4): $4x \equiv 2 \ (14)$ $(4,14) = 2$, $2 \mid 2$

$\Leftrightarrow$ 1st Solve $\underline{2x \equiv 1 \ (7)}$ then get. ② solutions

$x \equiv 4 \ (7)$,

2 solutions: 4, $4 + \frac{14}{2}$

☆ $\boxed{\text{mod } 14}$ 4, 11. (mod 14)

$x \equiv a_i \; (\text{mod } m_i)$

$i = 1, \dots, k$

Theorem 25 (Chinese Remainder Theorem). *If the moduli are coprime in pairs (ie., $(m_i, m_j) = 1$ for $i \neq j$), then the system has a unique solution mod $m_1 m_2 \dots m_k$.*

Proof of Uniqueness. Suppose there are two solutions $x \equiv y \equiv a_1 \mod m_1$, $x \equiv y \equiv a_2 \mod m_2$, etc. Then $m_1 | (x-y)$, $m_2 | (x-y)$, etc. Since m's are relatively prime in pairs, their product $m_1 m_2 \dots m_k$ divides $x - y$ as well, so $x \equiv y \mod m_1 m_2 \dots m_k$. So solution, if exists, must be unique mod $m_1 m_2 \dots m_k$. ∎

Proof of Existence. Write solution as a linear combination of a_i

$$A_1 a_1 + A_2 a_2 + \dots + A_k a_k$$

Want to arrange so that mod a_i all the A_j for $j \neq i$ are $\equiv 0 \mod m$, and $A_i \equiv 1 \mod m_i$. Let

$$\begin{aligned} N_1 &= m_2 m_3 \dots m_k \\ N_2 &= m_1 m_3 \dots m_k \\ &\vdots \\ N_i &= m_1 m_2 \dots m_{i-1} m_{i+1} \dots m_k \end{aligned}$$

or

Let $N = \prod_{i=1}^{k} m_i$

$N_i = N / m_i$

So $(N_i, m_i) = 1$, since all the other m are coprime to m_i. Let H_i equal the multiplicative inverse of $N_i \mod m_i$, and let $A_i = H_i N_i$. Then, $A_i \equiv 0 \mod m_j$ for $j \neq i$ and $A_i \equiv 1 \mod m_i$. So now let

$$\begin{aligned} a &= A_1 a_1 + A_2 a_2 + \dots + A_k a_k \\ &= H_1 N_1 a_1 + H_2 N_2 a_2 + \dots + H_k N_k a_k \end{aligned}$$

Then if we take mod m_i all the terms except ith term will vanish (since $m_i | N_j$ for $j \neq i$). So

$$\begin{aligned} a &\equiv H_i N_i a_i \pmod{m_i} \\ &\equiv a_i \pmod{m_i} \end{aligned}$$

∎

Eg.

$$\begin{array}{lll} x \equiv 2 \mod 3, & N_1 = 5 \cdot 7 = 35 \equiv 2 \mod 3, & H_1 = 2 \\ x \equiv 3 \mod 5, & N_2 = 3 \cdot 7 = 21 \equiv 1 \mod 5, & H_2 = 1 \\ x \equiv 5 \mod 7, & N_3 = 3 \cdot 5 = 15 \equiv 1 \mod 7, & H_3 = 1 \end{array}$$

$X \equiv N_1 H_1 a_1 + N_2 H_2 a_2 + N_3 H_3 a_3 \; (\text{mod } m_1 m_2 m_3)$

$\equiv 2 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 3 + 1 \cdot 15 \cdot 5 \; (\text{mod } 105) \equiv 278 \; (105)$

$\equiv 68 \; (105)$

CRT Chinese Remainder Theorem /2/26/2015/ Lect. 09

Thm: Solving simultaneously

(★) $x \equiv a_1 (m_1) \quad x \equiv a_2 (m_2) \cdots \quad x \equiv a_k (m_k)$

~~where $(m_1, \cdots, m_k)$ — pairwise coprime~~

(★) has a unique solution $(\text{mod } m_1 \cdots m_k)$

crutial to have $(m_1, \cdots, m_k)$ — pairwise coprime

Note/ a_i's DONNOT MATTER ! for any a_i the system has a unique solution $(\text{mod } m_1 \cdots m_k)$

Note/ In number theory, while solving linear congruences, We really need "uniqueness" or "# of solutions" up to modulo integers!

The solution has form: Let $m = \prod_{i=1}^{k} m_i$, b_j is $\left(\frac{m}{m_j}\right)^{-1} (m_j)$

$$\boxed{x_0 = \sum_{j=1}^{k} \frac{m}{m_j} b_j a_j}$$

Note: the assumption in CRT is essential.

[Recall: ① $ax \equiv ay \ (m) \iff x \equiv y \ \left(\frac{m}{(a,m)}\right)$

② $ax \equiv ay \ (m)$, $(a,m)=1 \Rightarrow x \equiv y \ (m)$

$\boxed{③\ x \equiv y \ (m_i)\ i=1,2,\dots,r \text{ iff } x \equiv y \ ([m_1 \cdots m_r])}$]

Eg. Show: there is no x for which both $x \equiv 29 \ (52)$ & $x \equiv 19 \ (72)$

by ③ above, $x \equiv 29 \ (52 = 4 \cdot 13)$

$\iff x \equiv 29 \ (4)$ & $x \equiv 29 \ (13)$

$\iff x \equiv 1 \ (4)$ & $x \equiv 3 \ (13)$

$x \equiv 19 \ (72 = 8 \cdot 9)$

$\iff x \equiv 19 \ (8)$ $x \equiv 19 \ (9)$

$x \equiv 3 \ (8)$ & $x \equiv 1 \ (9)$

$\boxed{\text{for } x \equiv 1 \ (4) \ \& \ x \equiv 3 \ (8) \quad \text{NO such } x!}$

Eg: Determine if the system $x \equiv 3 \ (10)$, $x \equiv 8 \ (15)$, $x \equiv 5 \ (84)$ has a solution; if so, find them.

use ③: $x \equiv 3 \ (2^1 \cdot 5)$ | $x \equiv 8 \ (3^1 \cdot 5^1)$ | $x \equiv 5 \ (2^2 \cdot 3^1 \cdot 7^1)$

$\iff x \equiv 1 \ (2)$, $x \equiv 3 \ (5)$ | $\iff x \equiv 2 \ (3)$, $x \equiv 3 \ (5)$ | $\iff x \equiv 1 \ (2^2)$, $x \equiv 2 \ (3^1)$, $x \equiv 5 \ (7)$

Thus we modify the system into: "7" linear congruences.

Note that $(15, 84) = 3$, $(10, 84) = 2$, $(10, 15) = 5$

two linear agree   two linear agree   two linear agree

Consider powers of 2 first

① 2: from mod 10: $x \equiv 1 \ (2)$

② 2^2: from mod 84: $x \equiv 1 \ (2^2)$

consistent & ② implies ① $\boxed{\text{So}}$ ① can be dropped

$\boxed{\text{System}}$ $\Longleftrightarrow$ 4 conditions:

$$\left.\begin{aligned} x &\equiv 1 \ (4) \\ x &\equiv 2 \ (3) \\ x &\equiv 3 \ (5) \\ x &\equiv 5 \ (7) \end{aligned}\right\}$$

$4, 3$

all different powers of different primes

$\Rightarrow$ must be rel. prime!

So our CRT method works:

$$x \equiv 173 \ (420)$$

Too much computation!

Method 2

$x \equiv 3\ (10)$, $x \equiv 8\ (15)$, $x \equiv 5\ (84)$

A B C

starting from C: $x \equiv 5\ (84) \overset{\text{defn.}}{\Longleftrightarrow} x = 5 + 84u,\ u \in \mathbb{Z}$

B $\Leftrightarrow$ $\cancel{5} + 84u \equiv 8\ (15) \Leftrightarrow 84u \equiv 3\ (15)$

(& $(84, 15) = 3$ $\quad 3 \mid 3$ ✓)

So u is a soln. of $84u \equiv 3 (15)$ (we can solve)

& & u must satisfies $u \equiv 2 (5)$

$\Rightarrow u = 2 + 5v$

$\boxed{\text{So}}$ x must be of form: $5 + 84(2+5v)$

$= 173 + 420v$

A:

$x \equiv 3\ (10) \Rightarrow \underset{\underset{3}{\equiv}}{173} + 420v \equiv 3\ (10)$

$10 \mid 420 \Rightarrow$ so for any v, congruence works

$\Rightarrow$ infinitly many solutions: $x = 173 + 420v,\ v \in \mathbb{Z}$

$$
\begin{aligned}
x &= H_1 N_1 a_1 + N_2 H_2 a_2 + N_3 H_3 a_3 \pmod{m_1 m_2 m_3} \\
&= 2 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 3 + 1 \cdot 15 \cdot 5 \pmod{105} \\
&= 278 \pmod{105} \\
&\equiv 68 \pmod{105}
\end{aligned}
$$

i.e., for any $0 \le a_1 < m_1$, $0 \le a_2 < m_2$, $\vdots$, $0 \le a_k < m_k$ if $(m_i, m_j) = 1$ $(i \neq j)$ then we always have a solution.

There are $m_1 \cdot m_2 \cdots m_k$ choices of system.

Note: Assuming we have $m_1, m_2 \dots m_k$ that are relatively prime, the Chinese Remainder Theorem says that any choice of $a_1 \mod m_1$, $a_2 \mod m_2$, etc. gives rise to particular $x(a_1, a_2, \dots a_k, m_1, \dots m_k) \mod m_1 m_2 \dots m_k$. Number of choices that we have is $m_1 m_2 \dots m_k$, which agrees with number of integers mod $m_1 m_2 \dots m_k$.

Note: Now note that $x(a_1, a_2, \dots a_k, m_1, \dots m_k)$ is coprime to $m_1 m_2 \dots m_k$ if and only if $(a_i, m_i) = 1$. $x = \sum_{j=1}^{k} \frac{m}{m_j} b_j a_j$

- If x is coprime to $\prod m_i$ then it is relatively coprime to each of them, so since $x \equiv a_i \mod m_i$ we'll also have $(a_i, m_i) = 1$.
- Conversely if $(a_i, m_i) = 1$ for all i, then since $x \equiv a_i \mod m_i$, this implies that $(x_i, m_i) = 1$ holds for all i, so $(x, \prod m_i) = 1$ as well.

What is the number of x coprime to $\prod m_i$? (by definition this is $\phi(m_1 m_2 \dots m_k)$)

$$
\underbrace{(\text{\# of choices of } a_1)}_{\phi(m_1)} \underbrace{(\text{\# of choices of } a_2)}_{\phi(m_1)} \dots
$$

with each a_i coprime to m_i. This gives corollary that if m_i coprime in pairs, $\phi(\prod m_i) = \prod \phi(m_i)$. We can use this to understand $\phi(n)$ for any n. With m_i coprime in pairs,

$$
\begin{gathered}
n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \\
m_1 = p_1^{e_1}, \quad m_2 = p_2^{e_2} \dots \quad m_k = p_k^{e_k} \\
\phi(n) = \phi(p_1^{e_1}) \phi(p_2^{e_2}) \dots \phi(p_k^{e_k})
\end{gathered}
$$

All we need, then, is how to find $\phi(p^e)$.

Note

$x = \sum_{j=1}^{k} \frac{m}{m_j} b_j a_j$

$$
\begin{aligned}
\phi(p^e) &= \#\text{ of } \{x | 1 \le x \le p^e \text{ and } (x,p) = 1 \text{ and so } (x, p^e) = 1\} \\
&= p^e - p^{e-1} \\
&= p^{e-1}(p-1) \\
&= p^e \left(1 - \frac{1}{p}\right)
\end{aligned}
$$

$1, 2, 3, \ldots, p-1$

p^{e-1} $p+1, p+2, \ldots 2p-1$

$p^{e-1}(p-1)$

and so

$$
\begin{aligned}
\phi(n) &= p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1)\ldots p_k^{e_k-1}(p_k-1) \\
&= p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right) \\
&= n\prod_{p|n}\left(1-\frac{1}{p}\right)
\end{aligned}
$$

optional

Numerical Calculations for Algorithms

Want to do arithmetic modulo N (some large number). Benchmark = time to write down N, which is roughly the number of digits of $N = c\log N$ for some constant c.

Addition is $\log N$ steps/time
Multiplication is $\log^2 N$ steps/time in the simplest way

Karatsuba Multiplication This is a faster algorithm for multiplication (see `http://en.wikipedia.org/wiki/Karatsuba_algorithm#Algorithm`); reduces time to $(\log N)^{\log 3/\log 2}$

Multiplication can be further improved by using Fast Fourier Transforms to $\log N \mathrm{poly}(\log\log n)$.

Exponentiation - we want to compute $a^b \mod N$, with a at most N and b is also small ($\sim N$). Most obvious way would be repeated multiplication for $N\log^2 N$, but better to use repeated squaring. Write b in binary as

$$
\begin{aligned}
b &= b_r b_{r-1}\ldots b_0 \\
&= 2^r b_r + 2^{r-1}b_{r-1} + \cdots + b_0
\end{aligned}
$$

then compute $a^{2^0}, a^{2^1}, \ldots a^{2^r} \mod N$ by repeatedly squaring the previous one (at most $\log^2 N$ for each). Then take

$$
\left(a^{2^0}\right)^{b_0}\left(a^{2^1}\right)^{b_1}\left(a^{2^2}\right)^{b_2}\ldots\left(a^{2^r}\right)^{b_r}
$$

for a total of $\log b \log^2 N \sim \log^3 N$ steps.

Thm: $f(x)$ — fixed polynomial in $\mathbb{Z}[x]$, and let $N(m)$ denote the # of solutions of $f(x) \equiv 0 \ (m)$.

If $m = m_1 m_2$ where $(m_1, m_2) = 1$, then $N(m) = N(m_1) N(m_2)$

~~If $m = m_1 m_2$ where for~~

For any int. m, we have primary decomposition.

$m = \prod_p p^{\alpha(p)}$ then we have

$$N(m) = \prod N(p^{\alpha(p)})$$

Pf: This is a special case of Theorem:

$$x \equiv y \ (m_i), \quad i = 1, 2, \cdots, r \iff x \equiv y \ ([m_1, \cdots, m_r])$$

$$f(x) \equiv 0 \ (p^{\alpha(p)}), \quad p \mid m \iff f(x) \equiv 0 \ (m)$$

$\boxed{\text{Eg}}$: $f(x) = x^2 + x + 7$. | Find $\boxed{\text{all roots}}$ if there are any for the congruence: $f(x) \equiv 0 \ (15)$

$15 = 3^1 \cdot 5^1$. consider: A $\boxed{x^2 + x + 7 \equiv 0 \quad (3)}$

B $\boxed{x^2 + x + 7 \equiv 0 \quad (5)}$

A: Try $x \equiv \pm 1, 0$. $1^2 + 1 + 7 \equiv 0 \ (3)$ ✓ $(-1)^2 - 1 + 7 \not\equiv 0 \ (3)$ X

$0^2 + 0 + 7 \not\equiv 0 \ (3)$

B: Try. $x \equiv \pm 1\ \pm 2\ 0 \quad (5)$ NO solution !

A ⊕ B No solution

[eg] Solve congruences

$$x^2+2x-3 \equiv 0 \pmod 5$$

Note over $\mathbb{Z}$, we have $x^2+2x-3 = (x-1)(x+3)$

works for mod 5 as well !

So $x \equiv 1, -3 \bmod 5$ are solutions.

Then ~~[illegible]~~ $(x-1)$ & $(x+3)$ is a composite #

i.e., $(x-1)(x+3) \equiv 0 \quad (5)$

iff $5 \mid x-1$ or $5 \mid x+3$.

so if $5 \mid x-1$ then $x \equiv 1 \quad (5)$

if $5 \mid x+3$ then $x \equiv 3 \quad (5)$

∴ $x \equiv 1, -3 \quad (5)$ are only solutions.

[redacted] Lecture 10

Congruences mod Primes, Order, Primitive Roots

Continuation of Proof of Hensel's Lemma. By lemma,

$$f(a+tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$$

Now we want to have the right hand side $\equiv 0 \bmod p^{j+1}$.

$$f(a) + tp^j f'(a) \equiv 0 \mod p^{j+1} \leftrightarrow tf'(a) + \frac{f(a)}{p^j} \equiv 0 \mod p$$

this has a unique solution

$$t \equiv -\left(\frac{f(a)}{p^j}\boxed{\frac{1}{f'(a)}}\right) \mod p$$

Note $f'(a) \not\equiv 0$ (p). then we can take inverse (mod p)

and: $\boxed{a+tp^j} \equiv a + (-f(a)\overline{f'(a)}_p)$ $a+tp^j$ — soln. (p^{j+1})

Direct formula - start with solution a of $f(x) \equiv 0 \bmod p$, and we want a solution mod p^*. Set $a_1 = a$. * — some power

$$a_{j+1} = a_j - f(a_j)\overline{f'(a)} \pmod{p^{j+1}}$$

where $\overline{f'(a)}$ is an integer chosen once at the beginning of the algorithm, which only matters mod p. It's chosen such that $\overline{f'(a)}f'(a) \equiv 1 \bmod p$. Then $f(a_j) \equiv 0 \bmod p^j$ for $j \geq 1$ as long as $f'(a) \not\equiv 0 \bmod p$.

Eg. Solve the congruence $x^2 \equiv -1 \mod 125$. ($f(x) = x^2+1$, $f'(x) = 2x$). Mod 5: $2^2 \equiv -1 \mod 5$, so set $a = 2$. $f'(a) \equiv 4 \bmod 5$, so can choose $\overline{f'(a)} = -1$.

$$\begin{aligned}
a_1 &= 2 \pmod 5 \\
a_2 &= a_1 - f(a_1)\overline{f'(a)} \pmod{25} \\
&= 2 - (5)(-1) \pmod{25} \\
&= 7 \pmod{25} \\
a_3 &= a_2 - f(a_2)\overline{f'(a)} \pmod{125} \\
&= 7 - (50)(-1) \pmod{125} \\
&= 57 \pmod{125}
\end{aligned}$$

Congruences to prime modulus: Assume that all the coefficients of $f(x) = a_n x^n + a_{n-1}x^{n-1} \cdots + a_0$ are reduced mod p and also that $a_n \not\equiv 0 \bmod p$. By dividing out by a_n, can assume that $f(x)$ is monic (ie., highest coefficient is 1). We can also assume degree n of f is less than p. If not, can divide f by $x^p - x$ to get

$$\begin{aligned}
f(x) &= g(x)(x^p - x) + r(x) \text{ with } \deg(r(x)) < p \\
f(a) &= g(a)(a^p - a) + r(a) \equiv r(a) \mod p \text{ by Fermat}
\end{aligned}$$

so roots of $f(x) \bmod p$ are the same as the roots of $r(x) \bmod p$.

60 -15

Theorem 28. *A congruence $f(x) \equiv 0$ mod p of degree n has at most n solutions.*

Proof. (imitates proof that polynomial of degree n has at most n complex roots)

Induction on n: congruences of degree 0 and 1 have 0 and 1 solutions, trivially. Assume that it holds for degrees $< n$ $(n \geq 2)$

If it has no roots, then we're done. Otherwise, suppose it does have a root α. Dividing $f(x)$ by $x - \alpha$, we get $g(x) \in \mathbb{Z}[x]$ and a constant r such that $f(x) = g(x)(x - \alpha) + r$. Now if we plug in α we get $f(\alpha) = (\alpha - \alpha)g(\alpha) + r = r$, which means that $f(\alpha) = r$ and $f(x) = (x - \alpha)g(\alpha) + f(\alpha)$.

We know that $f(\alpha) \equiv 0$ mod p. If β is any other root of $f(x)$ then we plug β into the equation to get $f(\beta) = (\beta - \alpha)g(\beta) + f(\alpha)$. Mod p, $f(\beta) \equiv (\beta - \alpha)g(\beta)$ mod p, so $0 \equiv (\beta - \alpha)g(\beta)$. We also assume that $\beta \not\equiv \alpha$, so $g(\beta) \equiv 0$ mod p.

So β is a root of $g(x)$ as a solution of $g(x) \equiv 0$ mod p. We know that $g(x)$ has degree $n - 1$, so by induction hypothesis $g(x) \equiv 0$ mod p has at most $n - 1$ solutions, which by including α gives $f(x)$ at most n solutions. ■

Corollary 29. *If $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \equiv 0$ mod p has more than n solutions, then all $a_i \equiv 0$ mod p.*

Theorem 30. *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then $f(x) \equiv 0$ mod p has exactly n distinct solutions if and only if $f(x)$ divides $x^p - \cancel{p}\,x$ mod p. Ie., there exists $g(x) \in \mathbb{Z}[x]$ such that $f(x)g(x) = x^p - x$ mod p as polynomials (all coefficients mod p)*

Proof. Suppose $f(x)$ has n solutions. Then $n \leq p$ because only p possible roots mod p (ie., $\deg(f) \leq \deg(x^p - x)$). Divide $x^p - x$ by $f(x)$ to get

$$x^p - x = f(x)g(x) + r(x), \quad \deg(r) < \deg(f) = n$$

Now note, if α is a root of $f(x)$ mod p then plug in to get

$$\begin{aligned} \alpha^p - \alpha &= f(\alpha)g(\alpha) + r(\alpha) \\ &\equiv 0g(\alpha) + r(\alpha) \\ &\equiv r(\alpha) \quad \text{mod } p \end{aligned}$$

so α must be a solution to $r(x) \equiv 0$ mod p. Since $f(x)$ has distinct roots, we see that $r(x) \equiv 0$ mod p has n distinct solutions. But $\deg(r) < n$. So by corollary we must have $r(x) \equiv 0$ mod p as a polynomial (each coefficient is 0 mod p.) Ie., $x^p - p = f(x)g(x)$ mod p, and so $f(x)$ divides $x^p - x$.

Now suppose $f(x) | x^p - x$ mod p. Write $x^p - x \equiv f(x)g(x)$ mod p, where $f(x)$ is a monic of degree n and $g(x)$ is a monic of degree $p - n$. We want to show that $f(x)$ has n distinct solutions.

By previous theorem, $g(x)$ has at most $p-n$ roots mod p. If $\alpha \in 0, 1, \dots p-1$ is not a root of $g(x)$ mod p then $\alpha^p - \alpha \equiv f(\alpha)g(\alpha)$ mod p, which by Fermat $\equiv 0$. Since $g(\alpha) \not\equiv 0 \bmod p$, $f(\alpha) \equiv 0 \bmod p$. So since there are at least $p-(p-n)$ such α, we see that $f(x)$ has at least n distinct roots mod p. By the theorem, $f(x)$ has at most n roots mod $p \Rightarrow f(x)$ has exactly n distinct roots mod p. ■

Corollary 31. *If $d|p-1$ then $x^d \equiv 1$ mod p has exactly d distinct solutions mod p.*

Proof. $d|p-1$, so $x^{d} - 1|x^{p-1} - 1$ as polynomials. $p-1 = kd$, so $x^{kd} - 1 = (x^d-1)(x^{(k-1)d} \cdots + 1)$. So $x^d - 1|x(x^{p-1}-1) = x^p - x$. So has d solutions. ■

(Use Theorem 30

Corollary 32. *Another proof of Wilson's Theorem*

Proof. Let p be an odd prime. Let $f(x) = x(x-1)(x-2)\dots(x-p+1)$. This has deg p and p solutions mod p, so it must divide $x^p - x$ mod p. Both polynomials are monic of the same degree (p), so must be equal mod p.

$$x(x-1)\dots(x-(p-1)) \equiv x^p - x \mod p$$

Coefficient of x on the LHS is just $(-1)(-2)\dots(-(p-1)) = (-1)^{p-1}(p-1)! = (p-1)!$ since p is odd, and so $(p-1)! \equiv -1$ mod p (coefficient on RHS). ■

This tells us much more as well - eg., $1 + 2 + \cdots + p - 1 \equiv 0$ mod p for $p \geq 3$, and $(1)(2) + (1)(3) + \dots (2)(3) \cdots + (p-1)(p-2) \equiv 0$ mod p for $p \geq 5$.

If we have a product $f(x) = (x-\alpha_1)\dots(x-\alpha_n)$ then $f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \dots (-1)^n \sigma_n$. σ_i are elementary symmetric polynomials.

$$\begin{aligned}
\sigma_1 &= \sum \alpha_i \\
\sigma_2 &= \sum_{i<j} \alpha_i \alpha_j \\
\sigma_k &= \sum (\text{all products of } k \text{ roots } \alpha_i)
\end{aligned}$$

Question - We know by Euler that if $(n, 35) = 1$, then $n^{\phi(35)} = n^{24} \equiv 1$ mod 35. Can 24 be replaced by something smaller? Ie., what's the smallest positive integer N such that if $(n, 35) = 1$ then $n^N \equiv 1$ mod 35.

(Definition) Order: If $(a, m) = 1$ and h is the smallest positive integer such that $a^h \equiv 1$ mod m then say h is the **order** of a mod m. Written as $h = \text{ord}_m(a)$.

Lemma 33. *Let $h = \text{ord}_m(a)$. The set of integers k such that $a^k \equiv 1$ mod m is exactly the set of multiples of h.*

1. GCD and LCM

GCD - Greatest common divisor of two integers a and b, denoted by (a,b), is the largest divisors among all common divisors of a and b

- If $GCD(a,b)=1$, we say a and b are relatively prime or coprime.
- $(a,b)=xa+yb$. for some x,y (Euclidean Algorithm)

LCM - least common multiple of two integers a & b. denoted by $[a,b]$, is the least positive multiples among all multiples of a & b.

- If $d=GCD(a,b)$, then $[a,b]=\frac{|ab|}{d}$

Eg: Find $x,y \in \mathbb{Z}$ such that $25x+15y=(25,15)^2$

We can use Euclidean Algorithm to find g,h, such that $25g+15h=(25,15)$

	25	15
25	1	0
15	0	1
10	1	-1
5	-1	2

$5=(-1)25+2(15)$

$\Rightarrow 5^2=\left((-1)25+2(15)\right)^2$

$=25^2+4\cdot 15^2-4\cdot 15\cdot 25$

$=(25-4\cdot 15)25+(4\cdot 15)\cdot 15$

$=(-35)\cdot 25+(60)\cdot 15$

or $=(25)\cdot 25+(4\cdot 15-4\cdot 25)15$

$=(25)25+(-40)15$

- **Primes** | An integer $P \geq 1$ called a prime number or a prime if there is NO divisor d of P satisfies $1 < d < P$; A number $a > 1$ is NOT a prime, it is called a composite number

Thm's only true for prime | If $p \mid ab$, then $p \mid a$ or $p \mid b$

- Two important Theorems |

① $a^p \equiv a \pmod{p}$ for any integer a.

② $a^{\phi(m)} \equiv 1 \pmod{m}$ for all a, such that $(a, m) = 1$

- In mod m system, NOT every integer ($\neq 0$) has inverse if m is a composite number

eg $m = 6$. reduced system $= \{1, \cancel{2}, \cancel{3}, \cancel{4}, 5\}$, $\phi(m) = 2$

only integers a, where $a \equiv 1$ (6) or $a \equiv 5$ (6) have inverse (mod 6)

For: • $a \equiv 1 \pmod{6}$, $a^{-1} \equiv 1$ (6) ; $a \equiv 5 \pmod{6}$, $a^{-1} \equiv 5 \pmod{6}$

• $\begin{cases} a \equiv 2, 3, 4. \ (6) & \text{it does Not have inverse!} \\ \text{i.e. You cannot find int. } b \text{ s.t. } ab \equiv 1 \ (6) \end{cases}$

- In mod p system, where p is a prime, all integers N, $p \nmid N$; have inverse mod p i.e, Given $N \in \mathbb{Z}$, if $p \nmid N$, then

- For $p = 5$, find inverse of all integers N if their inverses exist (mod p)

$P=5$. Given N, if $P \nmid N$, then N^{-1} exists (mod 5)

$$\begin{cases} N \equiv 1 \ (5), & N^{-1} \equiv 1 \ (5) \\ N \equiv -1 \ (5), & N^{-1} \equiv -1 \ (5) \\ N \equiv 2 \ (5), & \text{then } N^{-1} \text{ has to be } -2 \ (5) \\ N \equiv -2 \ (5), & \text{then } N^{-1} \text{ has to be } 2 \ (5) \end{cases}$$

$\boxtimes$

So given an integer N.

1) $N = 5k$ — no inverse $k \in \mathbb{Z}$ mod 5

2) $N = 5k+1$ — inverse $5l+1$, (mod 5), $k, l \in \mathbb{Z}$

3) $N = 5k-1$ — inverse $5l-1$, (mod 5), $k, l \in \mathbb{Z}$

4) $N = 5k+2$ — — — $5l-2$, (mod 5), $k, l \in \mathbb{Z}$

5) $N = 5k-2$ — — — $5l+2$, (mod 5), $k, l \in \mathbb{Z}$

$\boxtimes$

Use GCD & Inverses to solve linear system

Chinese Remainder Theorem

$$(\star) \begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \\ \vdots \\ x \equiv a_n \ (m_n) \end{cases}$$

System of n linear congruences, $(m_i, m_j) = 1$ $\forall i \neq j$

It has a unique solution mod $m_1 m_2 \cdots m_n$)

eg. Solve the following linear congruences: i.e. find all integer solutions.

① $x \equiv 1 \ (2)$ ② $2x \equiv 2 \ (3)$ ③ $x \equiv 1 \ (27)$ ④ $x \equiv 5 \ (7)$

Transform the system into linear congruences form in $(\star)$, i.e. coef $\equiv 1 (m)$

$(m_i, m_j) = 1$

① $x \equiv 1\ (2)$ ✓ $\boxed{④\quad x \equiv 5\ (7)}$ ✓ ④

② $2x \equiv 2\ (3) \Rightarrow 2 \cdot 2x \equiv 2 \cdot 2\ (3) \Rightarrow x \equiv 1\ (3)$

③: $x \equiv 1\ (27) \Leftrightarrow \boxed{x \equiv 1 (3^3)}$

$$\begin{cases} x \equiv \overset{a_1}{1}\ (\overset{m_1}{2}) \\ x \equiv \overset{a_2}{1}\ (\overset{m_2}{27}) \\ x \equiv \overset{a_3}{5}\ (\overset{m_3}{7}) \end{cases}$$

Let $m = 2 \cdot 27$

Solution: $b = \sum_{i=1}^{n} A_i a_i$, $A_i = \underline{H_i M_i}$, $M = \prod_{i=1}^{n} m_i$ & $M_i = \frac{M}{m_i}$

unique (mod $m_1 m_2 \cdots m_n$) $H_i \equiv M_i^{-1}\ (m_i)$

So: $M = m_1 m_2 m_3 = 2 \cdot 27 \cdot 7 = 378$ $M_1 = \frac{M}{m_1} = 189$, $M_2 = \frac{M}{m_2} = 14$, $M_3 = \frac{M}{m_3} = 54$

Need find M_i^{-1} (mod m_i).

① 189^{-1} (mod 2) or find $189 H_1 \equiv 1\ (2) \Rightarrow H_1 \equiv 1\ (2)$ $H_1 = 1$

② 14^{-1} (mod 27) find $14 H_2 \equiv 1\ (27) \Rightarrow H_2 \equiv 2\ (27)$ $H_2 = 2$

③ 54^{-1} (mod 7) find $54 H_3 \equiv 1\ (7) \Rightarrow H_3 \equiv 3\ (7)$ $H_3 = 3$

So $b = 1 \cdot 189 \cdot 1 + 2 \cdot 14 \cdot 1 + 3 \cdot 54 \cdot 5 = 927$

all solutions: $927 + (2 \cdot 27 \cdot 7)k = 927 + 378k$

or $\boxed{171 + 378k}$

· Hensel's Lemma

Suppose $f(x) \in \mathbb{Z}[x]$, $f(a) \equiv 0 \pmod{p^j}$, and $f'(a) \not\equiv 0 \ (p)$

Then $\exists!\, t \pmod p$ s.t. $f(a+tp^j) \equiv 0 \pmod{p^{j+1}}$

Here $t \equiv -\left(\frac{f(p)}{p^j}\right) \cdot (f'(a))^{-1} \pmod p$

Application | WANT To find $x \equiv b\ (p^m)$ s.t. $f(b) \equiv 0\ (p^m)$

Start w/ Find a_1 s.t. $f(a_1) \equiv 0\ (p)$ & $f'(a_1) \not\equiv 0 (p)$

set $a_2 = a_1 - f(a_1)\overline{f'(a_1)} \pmod{p^2}$

$a_3 = a_2 - f(a_2)\overline{f'(a_1)} \pmod{p^3}$

$\vdots$

$a_m = a_{m-1} - f(a_{m-1})\overline{f'(a_1)} \pmod{p^m}$

$\overline{f'(a)} :=$ the inverse of $f'(a)$ in mod p

Note we always have $a_i \equiv a_j \pmod p$

then $f'(a_i) \equiv f'(a_j) \pmod p$

$\Rightarrow$ $f'(a_i)^{-1} \equiv f'(a_j)^{-1} \pmod p$

6

eg: Solve congruence, for $f(x) = x^5 + 5x^2 - x + 1$, $f(x) \equiv 0 \ (125)$ 5^3

$f'(x) = 5x^4 + 10x - 1$

Step 1 find solution for $f(x_0) \equiv 0 \ (5)$ & $f'(x_0) \not\equiv 0 \ (5)$.

$f(x) \equiv (x^5 - x) + x + 5x^2 - x + 1 \equiv x - 1 \ (5)$ and $f'(x) \equiv 1 \not\equiv 0 \ (5)$

Solution: $f(x) \equiv 0 \ (5)$ is $x \equiv 1 \ (5) = a_1$

and $f'(1) \not\equiv 0 \ (5)$

---

and $f'(x) =$

$(x^5 - x) + x + x^3 - 1$

$x^5 - 5x^2$

$x^5 \quad x^3 - 1$

$f(x) = x^5 + x^3 - 1$

$f(x) \equiv (x^5 - x) + x + x^3$

$3 + 2$

$\equiv x^3 + \cancel{x}$ (5)

2

$f'(x) \equiv 5x^4 + 3x^2 \ (5)$

$\equiv 3x^2$

2

$f(x) \equiv x(x^2 - 4) \equiv x(x-2)(x+2)$

7

Simplify "$f(x)$" when mod p ; $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_0$

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0 \pmod p$$

$$\equiv a_n \underbrace{\left(x^n + a_{n-1} a_n^{-1} x^{n-1} + \cdots + a_1 a_n^{-1} x + a_0 a_n^{-1} \right)}_{h(x)}$$

[use Euclidean Algorithm

if $n \geq p$

$h(x) = (x^p - x)\, g(x) + r(x)$

& $h(x) \equiv r(x) \mod p$

$\deg r(x) < p$]

$\equiv a_n r(x)$

So To find solu. for $f(x) \equiv 0 \pmod p$

$\Leftrightarrow$ find solu for $a_n r(x) \equiv 0 \pmod p$

$\Leftrightarrow$ - - - for $r(x) \equiv 0 \pmod p$ $\deg r < p$

$\Leftrightarrow$ - - for monic $\boxed{a_t^{-1} r(x)} \equiv 0 \pmod p$

use $r(x)$ to denote the monic polynomial

8

Thm: A congruence $f(x) \equiv 0 \mod (p)$ has at most $\deg r(x)$ many solutions

Thm. A congruence $f(x) \equiv 0 \mod (p)$ has distinct solutions $(\mathrm{mod}\ p) \iff r(x) \mid x^p - x$

Thm. If $d \mid p-1$, then $x^d \equiv 1 \pmod{p}$ has exactly d distinct solutions

Midterm Exam I

Spring 2015 MAT 311 Number Theory

March 9, 2015

- Last Name (print):
- First Name (print):
- ID number (print):

Instructions

- Please answer each question in the space provided, and write full solutions.
- Please show all work, explain your reasons, and state all theorems you appeal to.
- Unless otherwise marked, answers without justification will get little or no partial credit.
- Cross out anything the grader should ignore and circle or box the final answer.
- Do NOT round answers.
- No books, notes, or calculators are allowed while taking the exam.

Problem	Full Points	Scores
1	30	
2	30	
3	20	
4	20	

Question 1: (a) [10 pts] Compute $gcd(91, 112)$ using any algorithm at all (even being psychic, i.e.,no proof required just get the right answer).

(b) [20 pts] Find integers x and y such that $112x - 91y = 2 \cdot gcd(91, 112)$.

Question 2: [30 *pts*] Determine if the following linear congruence system has a solution. If so, find ALL integer solutions.

$$\begin{aligned} 3x &\equiv 7 (\text{mod } 19) \\ x &\equiv 26 (\text{mod } 17) \\ 2x &\equiv 3 (\text{mod } 5) \\ x &\equiv 4 (\text{mod } 10) \\ x &\equiv 1 (\text{mod } 3) \end{aligned}$$

Question 3: Let $f(x) \in \mathbb{Z}[x]$, $f(x) = x^{18} + 17x^3 + 16$

(a) [5 *pts*] Find all solutions of the congruence $f(x) \equiv 0 \bmod 17$;

(b) [15 *pts*] Find one solution of the congruence $f(x) \equiv 0 \bmod 17^3$;

Question 4: [20 *pts*] Let $f(x) = x^7 - 1$. Determine if $f(x) \equiv 0 \pmod{127}$ has distinct solutions $\pmod{127}$.

Lecture 12 Number Theory

By previous theorem, $g(x)$ has at most $p-n$ roots mod p. If $\alpha \in 0, 1, \ldots p-1$ is not a root of $g(x)$ mod p then $\alpha^p - \alpha \equiv f(\alpha)g(\alpha)$ mod p, which by Fermat $\equiv 0$. Since $g(\alpha) \not\equiv 0$ mod p, $f(\alpha) \equiv 0$ mod p. So since there are at least $p-(p-n)$ such α, we see that $f(x)$ has at least n distinct roots mod p. By the theorem, $f(x)$ has at most n roots mod $p \Rightarrow f(x)$ has exactly n distinct roots mod p. ∎

Corollary 31. *If $d|p-1$ then $x^d \equiv 1$ mod p has exactly d distinct solutions mod p.*

Proof. $d|p-1$, so $x^{d-1}-1|x^{p-1}-1$ as polynomials. $p-1 = kd$, so $x^{kd}-1 = (x^d-1)(x^{(k-1)d}\cdots+1)$. So $x^d-1|x(x^{p-1}-1) = x^p - x$. So has d solutions. ∎

Corollary 32. *Another proof of Wilson's Theorem*

Proof. Let p be an odd prime. Let $f(x) = x(x-1)(x-2)\ldots(x-p+1)$. This has deg p and p solutions mod p, so it must divide $x^p - x$ mod p. Both polynomials are monic of the same degree (p), so must be equal mod p.

$$x(x-1)\ldots(x-(p-1)) \equiv x^p - x \mod p$$

Coefficient of x on the LHS is just $(-1)(-2)\ldots(-(p-1)) = (-1)^{p-1}(p-1)! = (p-1)!$ since p is odd, and so $(p-1)! \equiv -1$ mod p (coefficient on RHS). ∎

This tells us much more as well - eg., $1+2+\cdots+p-1 \equiv 0$ mod p for $p \geq 3$, and $(1)(2)+(1)(3)+\ldots(2)(3)\cdots+(p-1)(p-2) \equiv 0$ mod p for $p \geq 5$.

If we have a product $f(x) = (x-\alpha_1)\ldots(x-\alpha_n)$ then $f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \ldots (-1)^n \sigma_n$. σ_i are elementary symmetric polynomials.

$$\begin{aligned}
\sigma_1 &= \sum \alpha_i \\
\sigma_2 &= \sum_{i<j} \alpha_i \alpha_j \\
\sigma_k &= \sum (\text{all products of } k \text{ roots } \alpha_i)
\end{aligned}$$

Question - We know by Euler that if $(n, 35) = 1$, then $n^{\phi(35)} = n^{24} \equiv 1$ mod 35. Can 24 be replaced by something smaller? Ie., what's the smallest positive integer N such that if $(n, 35) = 1$ then $n^N \equiv 1$ mod 35.

(Definition) Order: If $(a, m) = 1$ and h is the smallest positive integer such that $a^h \equiv 1$ mod m then say h is the **order** of a mod m. Written as $h = \mathrm{ord}_m(a)$.

Lemma 33. *Let $h = \mathrm{ord}_m(a)$. The set of integers k such that $a^k \equiv 1$ mod m is exactly the set of multiples of h.*

Proof. $a^{rh} \equiv (a^h)^r \equiv 1^r \equiv 1 \bmod m$. Suppose we have k such that $a^k \equiv 1 \bmod m$. Want to show $h|k$. Write $k = hq + r$ where $0 \leq r < h$. $1 \equiv a^k = a^{hq+r} = a^{hq}a^r \equiv 1a^r \equiv a^r \bmod m$, so $a^r \equiv 1 \bmod m$. But $r < h$. So if $r > 0$, contradicts minimality of h, which means that $r = 0$, and k is multiple of h. ∎

Lemma 34. *If $h = \mathrm{ord}_m(a)$ then a^k has order $\frac{h}{(k,h)}$ mod m.*

Proof.

$$\begin{aligned} a^{kj} &\equiv 1 \mod m \\ &\leftrightarrow h|kj \\ &\leftrightarrow \frac{h}{(h,k)} \Big| \frac{k}{(h,k)} j \\ &\leftrightarrow \frac{h}{(h,k)} \Big| j \end{aligned}$$

So smallest such positive $j = \frac{h}{(h,k)}$. ∎

Lemma 35. *If a has order h mod m and b has order k mod m, and $(h,k) = 1$, then ab has order hk mod m.*

Proof. We know

$$\begin{aligned} (ab)^{hk} &\equiv (a^h)^k (b^k)^h \\ &\equiv 1^k 1^h \\ &\equiv 1 \mod m \end{aligned}$$

Conversely suppose that $r = \mathrm{ord}_m(ab)$.

$$\begin{aligned} (ab)^r &\equiv 1 \mod m \\ (ab)^{rh} &\equiv 1 \mod m \\ (a^h)^r b^{rh} &\equiv 1 \mod m \\ b^{rh} &\equiv 1 \mod m \end{aligned}$$

so $k|rh \Rightarrow k|r$ (since $(k,h) = 1$), and similarly $h|r$. So $hk|r$, and so $hk = \mathrm{ord}_m(ab)$. ∎

(Definition) Primitive Root: If a has order $\phi(m)$ mod m, we say that a is a **primitive root** mod m.

Eg. mod 7:

In mod 7:

1	has order	1		
2	has order	3		($2^3 \equiv 1 \bmod 7$)
3	has order	6	✓	($\phi(7) = 6$)
4	has order	3		
5	has order	6	✓	($\phi(7) = 6$)
6	has order	2		

Lemma 36. *Let p be prime and suppose $q^e \| p-1$ for some other prime q. Then there's an element mod p of order q^e.*

Assuming Lemma...

$$p - 1 = q_1^{e_1} q_2^{e_2} \dots q_r^{e_r}$$

Lemma says that $\exists\, g_1$ with $\mathrm{ord}_p(g_1) = q_1^{e_1}$, g_2 with $\mathrm{ord}_p(g_2) = q_2^{e_2}$, etc. Set $g = g_1 g_2 \dots g_r$. So by previous lemma above, g has order $q_1^{e_1} q_2^{e_2} \dots q_r^{e_r} = p - 1$ because all q_i are coprime in pairs. $p - 1 = \phi(p)$, so g is a primitive root mod p.

Proof. Consider solutions of $x^{q^e} \equiv 1 \bmod p$. Because $q^e | p-1$, $x^{q^e} - 1$ has exactly q^e roots mod p. If α is any such root, then $\mathrm{ord}_p(\alpha)$ must divide q^e.

So if it's not equal to q^e, it must divide q^{e-1}. Then α would have to be root of $x^{q^{e-1}} - 1 \equiv 0 \bmod p$, which has exactly q^{e-1} solutions. Since $q^e - q^{e-1} > 0$, there exists α such that $\mathrm{ord}_p(\alpha) = q^e$. ■

<u>Note</u>:

If $x^{q^e} \equiv 1 \pmod p$ & $q^e | p-1 \Rightarrow x^{q^e} - 1$ has q^e distinct roots mod p;

$\Rightarrow \#\{\alpha : \alpha^{q^e} \equiv 1 \ (p)\} = q^e$

If α has order $< q^e$ ~~...~~, then $\mathrm{order}_p(\alpha) | q^e$

indicates $\mathrm{order}_p(\alpha) = q^{e-1-N}$ $\quad N \in \mathbb{Z}_+ \cup \{0\}$

<u>since</u> $\mathrm{order}_p(\alpha) | q^{e-1-N} \Rightarrow \alpha$ is a root of $x^{q^{e-1}} \equiv 1$ or $\left((\alpha^{q^{e-1-N}})^{q^N} \equiv 1 \ (p) \right)$

& $\#\{\alpha : \alpha^{q^{e-1}} \equiv 1 \ (p)\} = q^{e-1}$

has to be an α <u>s.t.</u> $\mathrm{order}_p(\alpha) = q^e$

Lecture 13. Number Theory 03/26/2015

- Recall: Definition of order in mod m system

If $(a, m)=1$ and h is the smallest positive int. s.t.

$a^h \equiv 1 \pmod{m}$ then we say h is the order of a.

write $h = ord_m(a)$

$\boxed{eg}$: Let $m=5$.

for $a \equiv 4 \pmod 5$

we want to find $ord_5(4)$

$4^1 \equiv -1 \ (5)$ —

$4^2 \equiv 16 \ (5)$

$\equiv 1 \ (5)$ $\Rightarrow$ order of 4 mod 5 is

$2 < \phi(5)=4$ & $2 \mid \phi(5)$

- Defn: Primitive Root: If a has order $\phi(m) \pmod m$,

then we say a is a primitive root mod m

$\boxed{eg}$: Let $m=5$. for $a \equiv 4 \pmod 5$

since $ord_5(4) = 2 < \phi(5)$ $\Rightarrow$ $a \equiv 4 (5)$ NOT primitive

for $a \equiv 3 \pmod 5$. $a^3 \equiv 12 \pmod 5$

$a^2 \equiv 4 \pmod 5$ $a^4 \equiv 1 \pmod 5$

$\Big\}$ $a \equiv 3 (5)$ is a primitive root (mod 5)

In mod 7:

1	has order	1		
2	has order	3		($2^3 \equiv 1 \bmod 7$)
3	has order	6	✓	($\phi(7) = 6$)
4	has order	3		
5	has order	6	✓	($\phi(7) = 6$)
6	has order	2		

Lemma 36. *Let p be prime and suppose $q^e || p-1$ for some other prime q. Then there's an element mod p of order q^e.*

Assuming Lemma...

$$p - 1 = q_1^{e_1} q_2^{e_2} \dots q_r^{e_r}$$

Lemma says that $\exists\, g_1$ with $\mathrm{ord}_p(g_1) = q_1^{e_1}$, g_2 with $\mathrm{ord}_p(g_2) = q_2^{e_2}$, etc. Set $g = g_1 g_2 \dots g_r$. So by previous lemma above, g has order $q_1^{e_1} q_2^{e_2} \dots q_r^{e_r} = p - 1$ because all q_i are coprime in pairs. $p - 1 = \phi(p)$, so g is a primitive root mod p.

Proof. Consider solutions of $x^{q^e} \equiv 1 \bmod p$. Because $q^e | p-1$, $x^{q^e} - 1$ has exactly q^e roots mod p. If α is any such root, then $\mathrm{ord}_p(\alpha)$ must divide q^e.

So if it's not equal to q^e, it must divide q^{e-1}. Then α would have to be root of $x^{q^{e-1}} - 1 \equiv 0 \bmod p$, which has exactly q^{e-1} solutions. Since $q^e - q^{e-1} > 0$, there exists α such that $\mathrm{ord}_p(\alpha) = q^e$. ■

Note:

If $x^{q^e} \equiv 1 \pmod p$ & $q^e | p-1 \Rightarrow x^{q^e} - 1$ has

q^e distinct roots mod p;

$\Rightarrow \#\{\alpha : \alpha^{q^e} \equiv 1\ (p)\} = q^e$

If α has order $< q^e$, then $\mathrm{order}_p(\alpha) | q^e$

indicates $\mathrm{order}_p(\alpha) = q^{e-1-N}$ $\quad N \in \mathbb{Z}_+ \cup \{0\}$

since $\mathrm{order}_p(\alpha) | q^{e-1-N} \Rightarrow \alpha$ is a root of

$x^{q^{e-1}} \equiv 1$ or $\left(\left(\alpha^{q^{e-1-N}}\right)^{q^N} \equiv 1\ (p)\right)$

& $\#\{\alpha : \alpha^{q^{e-1}} \equiv 1\ (p)\} = q^{e-1}$

has to be an α s.t. $\mathrm{order}_p(\alpha) = q^e$

Lecture 13

Primitive Roots (Prime Powers), Index Calculus

Recap - if prime p, then there's a primitive root g mod p and it's order mod p is $p-1 = q_1^{e_1}q_2^{e_2}\dots q_r^{e_r}$. We showed that there are integers g_i mod p with order exactly $q_i^{e_i}$ (counting number of solutions to $x^{q_i^{e_i}} - 1 \equiv 0 \bmod p$). Set $g = \prod g_i$ - has order $\prod q_i^{e_i} = p-1$.

Number of primitive roots - suppose that m is an integer such that there is a primitive root g mod m. How many primitive roots mod m are there?

We want the order to be exactly $\phi(m)$. If we look at the integers 1, g, g^2, $\dots g^{\phi(m)-1}$, these are all coprime to m and distinct mod m. If we had $g^i \equiv g^j$ mod m $(0 \le i < j \le \phi(m)-1)$, then we'd have $g^{j-1} \equiv 1 \bmod m$ with $0 \le j-i < \phi(m)$, contradicting the fact that g is a primitive root.

Since there are $\phi(m)$ of these integers, they must be all the reduced residue classes mod m (in particular if $m = p$, a prime, then $\{1, 2, \dots p-1\}$ is a relabeling of $\{1, g, \dots g^{p-2}\}$ mod p). Suppose that a is a primitive root mod m, then $a \equiv g^k$ mod m. Recall that order of g^k is

$$\frac{\mathrm{ord}(g)}{(k, \mathrm{ord}(g))} = \frac{\phi(m)}{(k, \phi(m))}$$

So only way for the order to be exactly $\phi(m)$ is for k to be coprime to $\phi(m)$. Ie., the number of primitive roots mod m is exactly $\phi(\phi(m))$ if there's at least one. In particular, if $m =$ a prime, then number of primitive roots is $\phi(p-1)$.

eg $p=7$ $\phi(7-1) = \phi(6) = \phi(2)\,\phi(3) = 2$, $a \equiv 3, 5 \pmod 7$

Conjecture 37 (Artin's Conjecture). *Let a be a natural number, which is not a square. Then there are infinitely many primes p for which a is a primite root mod p.*

This is an open question. Hooley proved this conditional on GRH, and Heath-Brown showed that if a is a prime, then there are at most 2 values of a which fail the conjecture

(Definition) Discrete Log: Say p is a prime, and g is a primitive root mod p (ie., $1, g, g^2 \dots g^{p-2}$ are all the nonzero residue classes mod p). Say we have $a \not\equiv 0$ mod p. We know $a \equiv g^k$ for some k $(0 \le k \le p-2)$ - k is called the **index** or the **discrete log** of a to the base g mod p. This is a computationally hard problem, and is also used in cryptography.

Index Calculus - Let's say we're trying to solve a congruence $x^d \equiv 1 \bmod p$. Any x which satisfied this congruence is coprime to p. So if g is a primitive root

Goal find all k (mod p)

mod p, we can write $x \equiv g^k \bmod p$. New variable is now k:

$$
\begin{aligned}
x^d \equiv 1 \quad \bmod p &\longleftrightarrow g^{kd} \equiv 1 \quad \bmod p \\
&\longleftrightarrow p-1 = \operatorname{ord}(g) \text{ divides } kd \\
&\longleftrightarrow \frac{p-1}{(d,p-1)} \text{ divides } \frac{d}{(d,p-1)}k \\
&\longleftrightarrow \frac{(p-1)}{(d,p-1)} \text{ divides } k
\end{aligned}
$$

Note k is a variable

Key: Try to solve $x^2 \equiv 1 \pmod p$

if $p \neq 2$, then $(2, p-1) = 2$

$\Rightarrow$ 2 solutions!

± 1

So set of solutions for k is exactly the set of multiples of $\frac{(p-1)}{(d,p-1)}$ (remember k is only modulo $p-1$). So we can get all the solutions x by raising g to the exponent k, where $0 \leq k < p-1$ is a multiple of $\frac{p-1}{(d,p-1)}$. The number of solutions is

$$
\frac{(p-1)}{\frac{p-1}{(d,p-1)}} = \boxed{(d,p-1)}
$$

Similarly, if we're trying to solve the congruence $x^d \equiv a \bmod p$ ($a \not\equiv 0 \bmod p$), we can write $a \equiv g^l \bmod p$ so if $x \equiv g^k$ as before then $g^{kd} \equiv g^l \bmod p$. This means that $g^{kd-l} \equiv 1 \bmod p \leftrightarrow p-1 | kd - l \leftrightarrow kd \equiv l \bmod p-1$ (k is variable), which has a solution iff $(d, p-1)$ divides l, in which case it has exactly $(d, p-1)$ solutions.

Note:

$$
\begin{aligned}
(d,p-1) \text{ divides } l &\longleftrightarrow p-1 \text{ divides } \frac{l(p-1)}{(d,p-1)} \\
&\longleftrightarrow g^{l\frac{p-1}{(d,p-1)}} \equiv 1 \quad \bmod p \\
&\longleftrightarrow a^{\frac{p-1}{(d,p-1)}} \equiv 1 \quad \bmod p
\end{aligned}
$$

Note if $a \equiv g^l \pmod p$ & $\operatorname{ord}_p(g) = p-1$ then $\operatorname{ord}_p(g^l) = \frac{p-1}{(l, p-1)}$

Theorem 38. *There's a primitive root mod m iff $m = 1, 2, 4, p^e$, or $2p^e$ (where p is an odd prime). Let's assume that p is an odd prime, and $e \geq 2$. Want to show that there's a primitive root mod p^e.*

Part 1 - There's a primitive root mod p^2

Proof. Choose g to be a primitive root mod p, and use Hensel's Lemma to show there's a primitive root mod p^2 of the form $g + tp$ for some $0 \leq t \leq p-1$. We know $(g+tp, p) = 1$ since $p \nmid g$ and $p | tp$. $\operatorname{ord}_{p^2}(g+tp)$ must divide $\phi(p^2) = p(p-1)$.

On the other hand, if $(g+tp)^k \equiv 1 \bmod p^2$ then $(g+tp)^k \equiv 1 \bmod p \Leftrightarrow g^k \equiv 1 \bmod p \Leftrightarrow p - 1 | k$.

So $p-1$ divides $\operatorname{ord}_p(g+tp)$. Since $\operatorname{ord}_p(g+tp)$ is a multiple of $p-1$ and divides $p(p-1)$, it's either equal to $p-1$ or equal to $p(p-1) = \phi(p^2)$. We'll show that there's exactly one value of t for which the former happens.

Since there are p possible values of $t (0 \leq t \leq p-1)$, any of these remaining ones give a $g + tp$ which is a primitive root mod p^2. Consider $f(x) = x^{p-1} - 1$: mod p it has the root g. Since $f'(x) = (p-1)x^{p-2}$ and $f'(g) = (p-1)g^{p-2} \not\equiv 0 \bmod p$, by Hensel's Lemma there is a unique lift $g + tp$ of g mod p^2 satisfying $x^{p-1} \equiv 1$ mod p^2. This is the unique lift for which order is $p-1$ mod p^2. This proves that there's a primitive root mod p^2. □

Part 2 - Let g be a primitive root mod p^2. Then g is a primitive root mod p^e for every $e \geq 2$.

Proof. Since $\operatorname{ord}_{p^e}(g)$ divides $\varphi(p^e) = p^{e-1}(p-1)$ and also that $p-1 | \operatorname{ord}_{p^e}(g)$ (as in proof of previous part), $\operatorname{ord}_{p^e}(g)$ must be $p^k(p-1)$ for some $0 \leq k \leq e-1$. We want to show that $k = e-1$. To see that, it's enough to show that $g^{p^{e-2}(p-1)} \not\equiv 1$ mod p^e.

We'll show it by induction (base case is $e = 2$). $g^{p-1} \not\equiv 1 \bmod p^2$ is true because g is a primitive root mod p^2, so order $= p(p-1)$. So say we know it for e.

We know that $\phi(p^{e-1}) = p^{e-2}(p-1)$. So $g^{\phi(p^{e-1})} \equiv 1 \bmod p^{e-1}$ assuming that $g^{\phi(p^{e-1})} \not\equiv 1 \bmod p^e$. In other words $g^{\phi(p^{e-1})} = 1 + bp^{e-1}$ with $p \nmid b$. Need to show it for $e+1$ - ie., $g^{\phi(p^e)} \not\equiv 1 \bmod p^{e+1}$.

We know that $g^{p^{e-2}(p-1)} = 1 + bp^{e-1}$. Raising to power p we get

$$\begin{aligned}
g^{p^{e-1}(p-1)} &= (1 + bp^{e-1})^p \\
&= 1 + pbp^{e-1} + \binom{p}{2}(bp^{e-1})^2 + \binom{p}{3}(bp^{e-1})^3 + \dots \\
&\equiv 1 + bp^e \mod p^{e+1}
\end{aligned}$$

(because for $e \geq 2$, $3e-3 \geq e+1$ and $p|\binom{p}{2}$ so $\binom{p}{2}b^2p^{2e-2}$ divisible by p^{2e-1} and $2e-1 \geq e+1$).

So $g^{p^{e-1}(p-1)} \equiv 1 + bp^e \bmod p^{e+1}$ with $p \nmid b$, which $\not\equiv 1 \bmod p^{e+1}$. Completes the induction. □

Main Proof. Check 1, 2, 4 directly. p odd, $m = p^e$ proved. $m = 2p^e$ (p odd) - $\phi(m) = \phi(2)\phi(p^e) = \phi(p^e)$. Let g be a primitive root mod p^e. If g is odd, it is a primitive root mod m. If not odd, then add p^e to it.

Now show that nothing else works: otherwise, if $n = mm'$ with m and m' coprime and $m, m' > 2$, we'll show there does not exist a primitive root mod m. By hypothesis ($m, m' > 2$) we know $\phi(m)$ and $\phi(m')$ are even. So for $(a, n) = 1$, we have $(a,m) = 1 = (a,m')$. So $a^{\phi(m)} \equiv 1 \bmod m$ and $a^{\phi(m')} \equiv 1 \bmod m'$. So

$$\begin{aligned} a^{\phi(m)\phi(m')/2} &\equiv (a^{\phi(m)})^{\phi(m')/2} \\ &\equiv 1 \mod m \\ a^{\phi(m)\phi(m')/2} &\equiv 1 \mod m' \\ \text{Similarly so, } a^{\phi(m)\phi(m')/2} &\equiv 1 \mod n \end{aligned}$$

but $\phi(n) = \phi(m)\phi(m')$ so $\operatorname{ord}_n(a) < \phi(n)$. So a can't be a primitive root mod n.

Only remaining candidate is $n = 2^k$ for $k \geq 3$. No primitive root mod 8 since $\text{odd}^2 \equiv 1 \bmod 8$ (and $\phi(8) = 4$). So if a is odd, $a^2 = 1 + 8k$. Show by induction that $a^{2^{k-2}} \equiv 1 \bmod 2^k$ ($k \geq 3$). Since $\phi(2^k) = 2^{k-1}$, we see there does not exist a primitive root mod 2^k.

■

Lect. 15 | Thu. 4/2/2015

Recall :

$m = p_1^{e_1} \cdots p_k^{e_k}$

$\phi(m) = \phi(p_1^{e_1}) \cdots \phi(p_k^{e_k}) = p_1^{e_1-1}(p_1-1) \cdots p_k^{e_k-1}(p_k-1).$

1). If g is a primitive root mod p

<u>then</u> $\{1, g, g^2, \cdots, g^{p-2}\}_{\text{mod } p} = \{1, 2, \cdots, p-1\}_{\text{mod } p}$

2). If $\exists$ primitive root g (mod m) where m is composite.

<u>then</u> there are $\phi(m)$ of integers: in $\{1, g, g^2, \cdots, g^{\phi(m)-1}\}_{\text{mod } m}$

& $\{1, g, g^2, \cdots, g^{\phi(m)-1}\}_{\text{mod } m} = \{a \mid (a, m) = 1, 1 \le a < m\}$

& there are $\phi(\phi(m))$ many

3). $x^d \equiv 1 \pmod p$ has: $(d, p-1)$ many roots.

4). <u>Thm</u> (w/o proof) There is a primitive root mod m.

iff $m = 1, 2, 4, p^n$ (p-odd, $n \ge 1$), $2p^m$ (p-odd. $m \ge 1$)

<u>Non-example</u>: $m = 8$, $1, 3, 5, 7$

$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1$ mod 8.

So none generate.

eg: Determine if there are primitive roots mod 18. if so how many?

$18 = 2\cdot 3^2 \Rightarrow$ there are primitive roots mod 18)

$\#$ primitive roots $= \phi(\phi(18)) = \phi(\phi(2)\cdot\phi(3^2)) = \phi(1\cdot 3\cdot(3-1))$
$= \phi(3\cdot 2) = 2\cdot 1 = 2.$

eg: Determine # of solutions of $x^{15} \equiv 1 \mod (7)$.

Note $x^7 \equiv x \pmod 7$

So $x^{15} \equiv (x^7)^2 \cdot x \equiv x^3 \equiv 1 \mod 7$

So # of solutions $= (3, 7-1) = (3, 6) = 3$

Note $(15, 7-1) = 3$ you can use $(d, p-1)$ directly w/o reduce d to $d' < p$

Quadratic Residues, Quadratic Reciprocity

Quadratic Congruence - Consider congruence $ax^2 + bx + c \equiv 0 \mod p$, with $a \neq 0 \mod p$. This can be reduced to $x^2 + ax + b \equiv 0$, if we assume that p is odd (2 is trivial case). We can now complete the square to get

$$\left(x + \frac{a}{2}\right)^2 + b - \frac{a^2}{4} \equiv 0 \mod p$$

So we may as well start with $x^2 \equiv a \mod p$

If $a \equiv 0 \mod p$, then $x \equiv 0$ is the only solution. Otherwise, there are either no solutions, or exactly two solutions (if $b^2 \equiv a \mod p$, then $x = \pm b \mod p$). ($x^2 \equiv a \equiv b^2 \mod p \Rightarrow p | x^2 - b^2 \Rightarrow p | (x-b)(x+b) \Rightarrow x \equiv b$ or $-b \mod p$). We want to know when there are 0 or 2 solutions.

(Definition) Quadratic Residue: Let p be an odd prime, $a \not\equiv 0 \mod p$. We say that a is a **quadratic residue** mod p if a is a square mod p (it is a **quadratic non-residue otherwise**).

Lemma 39. *Let $a \not\equiv 0 \mod p$. Then a is a quadratic residuemod p iff $a^{\frac{p-1}{2}} \equiv 1$ mod p*

Proof. By FLT, $a^{p-1} \equiv 1 \mod p$ and $p-1$ is even. This follows from index calculus. Alternatively, let's see it directly

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \mod p \Rightarrow a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$$

Let g be a primitive root mod p. $\{1, g, g^2 \dots g^{p-2}\} = \{1, 2, \dots p-1\} \mod p$. Then $a \equiv g^k \mod p$ for some k. With that $a = g^{k+(p-1)m} \mod p$ so k's only defined mod $p-1$. In particular, since $p-1$ is even, so we know k is even or odd doesn't depend on whether we shift by a multiple of $p-1$. (ie., k is well defined mod 2).

We know that a is quadratic residue mod p iff k is even (if $k = 2l$ then $a \equiv g^{2l} \equiv (g^l)^2 \mod p$). Conversely if $a \equiv b^2 \mod p$ and $b = g^l \mod p$ we get $a \equiv g^{2l}$ mod p, so k is even.

Note: this shows that half of residue class mod p are quadratic residues, and half are quadratic nonresidues. Now look at $a^{\frac{p-1}{2}} \equiv \left(g^k\right)^{\frac{p-1}{2}} \equiv g^{\frac{k(p-1)}{2}} \mod p$. $k \equiv 1 \mod p$ iff $p - 1 = \text{ord}_p\, g$ divides $\frac{k(p-1)}{2}$ iff $(p-1) | \frac{k(p-1)}{2} \leftrightarrow 2 | k \leftrightarrow a$ is a quadratic residue. ■

(Definition) Legendre Symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \mod p \\ -1 & \text{if } a \text{ is a quadratic non-residue} \mod p \end{cases}$$

Defined for odd prime p, when $(a,p) = 1$. (For convenience and clarity, written $(a|p)$).

We just showed that $(a|p) \equiv a^{\frac{p-1}{2}} \mod p$.

Remark 1. This formula shows us that $(a|p)(b|p) = (ab|p)$.

$$\text{LHS} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \mod p \equiv \text{RHS} \mod p$$

and since both sides are $\pm 1 \mod p$, which is an odd prime, they must be equal
Similarly, $(a^2|p) = (a|p)^2 = 1$

Eg. (

$$(-4|79) = (-1 \cdot 2^2|79) = (-1|79)(2|79)^2 = (-1|79) = (-1)^{39} = -1$$

Also, 79 is not $1 \mod 4$ so -1 is quadratic non-residue.

Eg2. $\left(\frac{24}{19}\right) \overset{\text{by def}}{=} \begin{cases} 1 & \text{if } \exists c \text{ s.t. } c^2 \equiv 24 \ (19) \\ -1 & \text{if } \nexists c \text{ s.t. } c^2 \equiv 24 \ (19) \end{cases}$

$= \left(\frac{24-19}{19}\right)$

$= \left(\frac{5}{19}\right)$

$= 5^{\frac{19-1}{2}} \ (19)$

$= 5^9 \ (19)$

$= 1$

We'll work toward quadratic reciprocity relating $(p|q)$ to $(q|p)$. We'll do Gauss's 3rd proof.

Lemma 40 (Gauss Lemma). *Let p be an odd prime, and $a \not\equiv 0 \mod p$. For any integer x, let x_p be the residue of $x \mod p$ which has the smallest absolute value. (Divide x by p, get some remainder $0 \le b < p$. If $b > \frac{p}{2}$, let $x_p = b$, if $b > \frac{p}{2}$, let x_p be $b - p$. ie., $-\frac{p}{2} < x_p < \frac{p}{2}$) Let n be the number of integers among $(a)_p, (2a)_p, (3a)_p \ldots ((\frac{p-1}{2})a)_p$ which are negative. Then $(a|p) = (-1)^n$.*

Proof. (Similar to proof of Fermat's little Theorem)

We claim first that if $1 \le k \ne l \le \frac{p-1}{2}$ then $(ka)_p \ne \pm(la)_p$. Suppose not true: $(ka)_p = \pm(la)_p$. Then, we'd have

$$ka \equiv \pm la \mod p \Rightarrow (k \mp l)a \equiv 0 \mod p \Rightarrow k \mp l \equiv 0 \mod p$$

This is impossible because $2 \le k + l \le p - 1$ and $-\frac{p}{2} < k - l < \frac{p}{2}$ and $k - l \ne 0$ (no multiple of p possible).

So the numbers $|(ka)_p|$ for $k = 1 \ldots \frac{p-1}{2}$ are all distinct mod p (there's $\frac{p-1}{2}$ of

2

them) and so must be the integers $\{1, 3 \ldots \frac{p-1}{2}\}$ in some order.

$$
\begin{aligned}
1 \cdot 2 \cdot \cdots \cdot \left(\frac{p-1}{2}\right) &\equiv \prod_{k=1}^{\frac{p-1}{2}} |(ka)_p| \mod p \\
&\equiv (-1)^n \prod_{k=1}^{\frac{p-1}{2}} (ka)_p \mod p \\
&\equiv (-1)^n \prod_{k=1}^{\frac{p-1}{2}} ka \mod p \\
&\equiv a^{\frac{p-1}{2}} (-1)^n \left(1 \cdot 2 \cdot \cdots \cdot \left(\frac{p-1}{2}\right)\right) \mod p \\
\Rightarrow 1 &\equiv a^{\frac{p-1}{2}} (-1)^n \mod p \\
a^{\frac{p-1}{2}} &\equiv (-1)^n \mod p \\
(a|p) &\equiv (-1)^n \mod p \\
(a|p) &= (-1)^n \text{ since } p > 2
\end{aligned}
$$

where the second step follows from the fact that exactly n of the numbers $(ka)_p$ are < 0. ■

Theorem 41. *If p is an odd prime, and $(a, p) = 1$, then if a is odd, we have $(a|p) = (-1)^t$ where $t = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor$. Also, $(2|p) = (-1)^{(p^2-1)/8}$*

Proof. We'll use the Gauss Lemma. Note that we're only interested in $(-1)^n$. We only care about $n \mod 2$.

We have, for every k between 1 and $\frac{p-1}{2}$

$$
\begin{aligned}
ka &= p \left\lfloor \frac{ka}{p} \right\rfloor + (ka)_p + \begin{cases} 0 & \text{if } (ka)_p > 0 \\ p & \text{if } (ka)_p < 0 \end{cases} \\
&\equiv \left\lfloor \frac{ka}{p} \right\rfloor + |(ka)_p| + \begin{cases} 0 & \text{if } (ka)_p > 0 \\ 1 & \text{if } (ka)_p < 0 \end{cases} \mod 2
\end{aligned}
$$

Sum all of these congruences mod 2

$$\sum_{k=1}^{(p-1)/2} ka \equiv \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{k=1}^{(p-1)/2} |(ka)_p| + n \mod 2$$

$$\begin{aligned}\sum_{k=1}^{(p-1)/2} ka &= a \sum_{k=1}^{(p-1)/2} k \\ &= \frac{1}{2} a \left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right) \\ &= \frac{a(p^2-1)}{8}\end{aligned}$$

Now $\sum |(a)_p|$. Since $\{|a|_p, \ldots, |\frac{p-1}{2}a|_p\}$ is just $\{1 \ldots \frac{p-1}{2}\}$,

$$\begin{aligned}\sum_{k=1}^{(p-1)/2} |(ka)_p| &= \sum_{k=1}^{(p-1)/2} k \\ &= \frac{1}{2}\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}\right) \\ &= \frac{p-1}{8}\end{aligned}$$

Plug in to get

$$\begin{aligned}n &\equiv a\left(\frac{p^2-1}{8}\right) - \left(\frac{p^2-1}{8}\right) + \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor \mod 2 \\ &\equiv (a-1)\left(\frac{p^2-1}{8}\right) + \sum_{k=1}^{(p-1)/2} (ka|p) \mod 2\end{aligned}$$

If a is odd, we have $\frac{p^2-1}{8}$ is integer and $a-1$ is even, so product $\equiv 0 \mod 2$, to get

$$\begin{aligned}n &\equiv \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor \mod 2 \\ &\equiv t \mod 2\end{aligned}$$

$$\text{So } (a|p) = (-1)^n = (-1)^t$$

When $a = 2$,

$$n \equiv \frac{p^2-1}{8} + \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2k}{p} \right\rfloor \mod 2$$

So, note that for $k \in \{1 \dots \frac{p-1}{2}\}$

$$2 \le 2k \le p-1$$

so

$$0 < \frac{2}{p} \le \frac{2k}{p} \le \frac{p-1}{p} < 1$$

so

$$\lfloor \frac{2k}{p} \rfloor = 0$$

so

$$\sum_{k=1}^{(p-1)/2} (2k|p) = 0$$

so

$$n \equiv \frac{p^2-1}{8} \mod p \text{ and } (2|p) = (-1)^n = (-1)^{\frac{p^2-1}{8}}$$

So far,

$$(-1|p) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p = 1 \mod 4 \\ -1 & \text{if } p = 3 \mod 4 \end{cases}$$

Check

$$(2|p) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p = 1,7 \mod 8 \\ -1 & \text{if } p = 3,5 \mod 4 \end{cases}$$

■

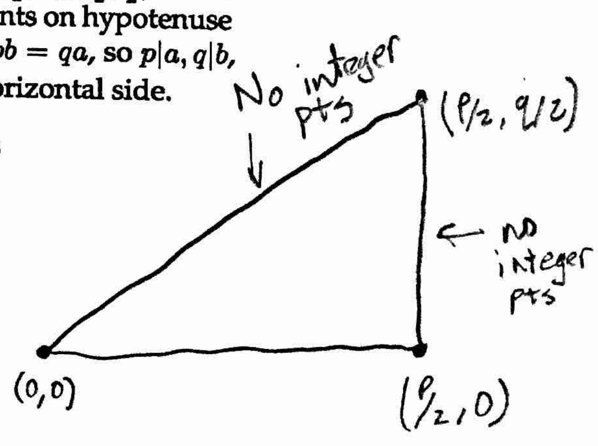
Theorem 42 (Quadratic Reciprocity Law). *If p, q are distinct odd primes, then*

$$(p|q)(q|p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1 & \text{if } p \text{ or } q \equiv 1 \mod 4 \\ -1 & \text{otherwise} \end{cases}$$

Proof. Consider the right angled triangle with vertices $(0,0), (\frac{p}{2}, 0), (\frac{p}{2}, \frac{q}{2})$. Note that: no integer points on vertical side, no nonzero integer points on hypotenuse (slope is $\frac{q}{p}$, so if we had integer point (a,b) then $\frac{b}{a} = \frac{q}{p} \Rightarrow pb = qa$, so $p|a, q|b$, and if $(a,b) \neq (0,0)$, then $a \ge p, b \ge q$). Ignore the ones on horizontal side.

Claim: the number of integer points on interior of triangle is

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor$$



Proof. If we have a point (k, l), then $1 \leq k \leq \frac{p-1}{2}$ and slope $\frac{l}{k} < \frac{q}{p} \Rightarrow l < \frac{qk}{p}$. Number of points on the segment $x = k$ is the number of possible l, which is just $\left\lfloor \frac{qk}{p} \right\rfloor$. $\square$

Add these (take triangle, rotate, add to make rectangle) - adding points in interior of rectangle is

$$\sum_{l=1}^{(p-1)/2} \left\lfloor \frac{pl}{q} \right\rfloor + \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$$

$$(q|p) = (-1)^{t_1} \text{where } t_1 = \sum \left\lfloor \frac{qk}{p} \right\rfloor$$

$$(p|q) = (-1)^{t_2} \text{where } t_2 = \sum \left\lfloor \frac{pl}{q} \right\rfloor$$

$$(p|q)(q|p) = (-1)^{t_1+t_2} \text{where } t_1 + t_2 = \text{ total number of points}$$

$\blacksquare$

Defined the Jacobi Symbol - used to compute Legendre Symbol efficiently (quadratic character)

Eg.

$$\begin{aligned}(1729|223) &= (168|223) = (4 \cdot 42|223) = (42|223)\\ &= (2|223)(21|223) = (21|223) = (223|21) = (13|21)\\ &= (21|13) = (8|13) = (2|13) = -1\end{aligned}$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} -1 & p,q \equiv 3\ (4) \\ 1 & \text{else} \end{cases}$$

$$(-1|p) = \begin{cases} -1 & \text{if } p \equiv 3 \mod 4 \\ 1 & \text{if } p \equiv 1 \mod 4 \end{cases}$$

$$(2|p) = \begin{cases} -1 & \text{if } p \equiv \pm 3 \mod 8 \\ 1 & \text{if } p \equiv \pm 1 \mod 8 \end{cases}$$

Lemma 43. *If p, q, r are distinct odd primes, and $q \equiv r \mod 4p$, then $(p|q) = (p|r)$.*

Proof. We know $(q|p) = (r|p)$ since $q \equiv r \mod p$. Also, q and r are both either 1 mod 4 or both 3 mod 4. So

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{r-1}{2}}$$

$$\begin{aligned}(p|q) &= (q|p)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\\ &= (r|p)(-1)^{\frac{p-1}{2}\frac{r-1}{2}}\\ &= (p|r)\end{aligned}$$

■

Eg. Characterize the primes p for which 17 is a square mod p. It's clear that 17 is square mod 2. We see that since $17 \equiv 1 \mod 4$, so if $q \equiv r \mod 17$ then $(17|q) = (17|r)$. So we only need to look mod 17 to see when $(17|q) = (q|17) = 1$. Go through mod 17: $\pm 1, \pm 2, \pm 4, \pm 8 \mod 17$ are nonzero square classes, so 17 is a square mod q iff $q = 2, 17$, or $\pm 1, \pm 2, \pm 4, \pm 8 \mod 17$.

If we had asked for 19, we need to look at classes mod $(4 \cdot 19)$, since $19 \not\equiv 1 \mod 4$. (If $q = 1 \mod 4$ then $(19|q) = (q|19)$, so we need q to be a square mod 19. If $q = 3 \mod 4$ then $(19|q) = -(q|19)$, we need q to be not square mod 19)

Euclidean gcd Algorithm - Given $a, b \in \mathbb{Z}$, not both 0, find (a, b)

Algorithm: Input: p - odd prime ; n — quadratic residue (p)

Output: An integer R. s.t. $R^2 \equiv n \ (p)$

steps 1): factor out powers of 2 from $p-1$, $p-1 = 2^S Q$ $\begin{cases} S=1 \Rightarrow p \equiv 3 \ (4) \Rightarrow R = \pm n^{\frac{p+1}{4}} \\ S \neq 1 \sim \end{cases}$

2). Select a z s.t. the Legendre symbol $\left(\frac{z}{p}\right) = -1$ (z - Quad. non residence) & set $c \equiv z^Q$

1. If $a, b < 0$, replace with negative
2. If $a > b$, switch a and b
3. If $a = 0$, return b
4. Since $a > 0$, write $b = aq + r$ with $0 \le r < a$. Replace (a, b) with (r, a) and go to Step 3.

3) Set $R \equiv n^{\frac{Q+1}{2}}$, $t = n^Q$, $M = S$

4) loop: if $t \equiv 1$ return R

Otherwise, find the lowest i, $0 < i < M$ s.t. $t^{2^i} \equiv 1$. (i.e. repeating squaring)

let $b \equiv c^{2^{M-i-1}}$, & $R = Rb$, $t = tb^2$, $c \equiv b^2$ & $M = i$

Only for prime modulo

Tonelli's Algorithm - To compute square roots mod p (used to solve $x^2 \equiv a \mod p$). Need a quadratic non-residue mod p, called n. Let g be a primitive root mod p. Now let $p - 1 = 2^s t$, for t odd. We know n is a power of g, say $n \equiv g^k$. Set $c \equiv n^t \equiv g^{kt}$.

Claim: The order of c is exactly 2^s.

Proof.

$$\begin{aligned} c^{2^s} &\equiv (g^{kt})^{2^s} \\ &\equiv (g^{t2^s})^k \\ &\equiv (g^{p-1})^k \\ &\equiv 1 \mod p \end{aligned}$$

So $\text{ord}(c)$ has to divide 2^s, so it's a power of 2. If we can show that $c^{2^{s-1}} \not\equiv 1 \mod p$ then order has to be 2^s.

$$\begin{aligned} c^{2^{s-1}} &\equiv (g^{kt})^{2^{s-1}} \\ &\equiv (g^{t2^{s-1}})^k \\ &\equiv (g^{(p-1)/2})^k \mod p \\ &\equiv (-1)^k \mod p, \text{ since } g \text{ is a primitive root} \end{aligned}$$

Note that k is odd since otherwise $n \equiv g^k$ would be a quadratic residue, so we get $c^{2^{s-1}} \equiv -1 \mod p$, proving claim that $\text{ord}(c) = 2^s$ ∎

Lemma 44. *If a, b are coprime to p and have order $2^j \mod p$ (for $j > 0$) then ab has order 2^k for some $k < j$.*

Proof. Since $a^{2^j} \equiv 1 \mod p$, $(a^{2^{j-1}})^2 \equiv 1 \mod p$, we have $a^{2j-1} \equiv \pm 1 \mod p$. So we must have $a^{2^{j-1}} \equiv -1 \mod p$, since $\text{ord}(a) = 2^j$. Similarly $b^{2^{j-1}} \equiv -1 \mod p$. Therefore, $(ab)^{2^{j-1}} \equiv 1 \mod p$, so order has to divide 2^{j-1}, so $k < j$. ∎

Proof of Tonelli's Algorithm. First check (by repeated squaring) if $a^{(p-1)/2} \equiv 1 \mod p$. If not, terminate with "false." So assume now on that $a^{(p-1)/2} \equiv 1 \mod p$.

Set $A = a$ and $b = 1$. At each step $a = Ab^2$ ($a \equiv Ab^2 \mod p$) At the end, want $A = 1$, so b is square root of $a \mod p$.

Each step: decrease the power of 2 dividing the order of A. To start with, $A^{(p-1)/2} = A^{2^{s-1}t} \equiv 1 \mod p$. Check if $A^{(p-1)/4} \equiv 1 \mod p$.

If not, then $A^{2^{s-2}t} \equiv -1 \mod p$ (since $(A^{2^{s-2}t})^2 \equiv 1 \mod p$). So powers of 2 dividing $\operatorname{ord}(A)$ is exactly 2^{s-1}. Same as the power of 2 diving ord $(c^2) = 2^{s-1}$. So set $A = Ac^{-2}, b = bc \mod p$. Notice that

$$\begin{aligned}(Ac^{-2})^{2^{s-2}t} &= \frac{A^{2^{s-2}t}}{c^{2^{s-1}t}} \\ &\equiv (-1)(-1)^t \\ &\equiv 1 \mod p\end{aligned}$$

ord (Ac^{-2}) divides $2^{s-2}t$, so power of 2 dividing the order is at most 2^{s-2}, so has decreased by 1.

If yes, (ie., $A^{2^{s-2}t} \equiv 1 \mod p$), do nothing.

Next step: check if $A^{2^{s-3}t} = A^{(p-1)/8} \equiv 1 \mod p$.

If no, (ie., $A^{2^{s-3}t} \equiv -1 \mod p$, set $A := Ac^{-4}$, $b := bc^2$ (c^4 has order 2^{s-2}). $(Ac^{-4})^{2^{s-3}t} \equiv 1$.

If yes, do nothing.

After at most s steps we'll reach the stage when $a \equiv Ab^2 \mod p$ and the power of 2 dividing $\operatorname{ord}(A)$ is 1 - ie., $\operatorname{ord}(A)$ is odd. Now we just compute a square root of A as follows: $\operatorname{ord}(A)$ odd and divides $p - 1 \equiv 2^s t$, so divides t. So $A^t \equiv 1 \mod p$ (t odd). Claim $A^{(t+1)/2}$ is a square root of $A \mod p$.

$$\begin{aligned}(A^{(t+1)/2})^2 &= A^{t+1} \\ &= A^t A \\ &\equiv 1 \cdot A \\ &\equiv A \mod p\end{aligned}$$

So algorithm just returns $bA^{(t+1)/2}$ as $\sqrt{a}$ ∎

$\boxed{\text{eg}}$: Solve congruence $x^2 \equiv 10 \pmod{13}$.

① since $10^{\frac{p-1}{2}} \equiv 10^6 \equiv 1 \pmod{13}$, 10 is a quad. residue

$\underline{\underline{\text{So}}}$ we have a solution;

① Observe: $p-1 = 12 = 2^2 \cdot 3$ $\underline{\underline{\text{So}}}$ $Q = 3$, $S = 2 > 1$

② Take $z = 2$ as the quadratic nonresidue (since $2^{\frac{13-1}{2}} \equiv -1 \ (13)$ — Euler's criterion

$\left(\text{or } \left(\frac{2}{p}\right) = \begin{cases} -1 & \text{if } p \equiv \pm 3 \ (8) \\ 1 & \text{if } p \equiv \pm 1 \ (8) \end{cases} \right)$)

Let $c = 2^3 \equiv 8 \ (13)$.

③: $R = 10^{\frac{3+1}{2}} \equiv -4 \ (13)$, $t = 10^3 \equiv -1 \ (13)$ $M = 2$

④: Start loop: $t \equiv -1 \not\equiv 1 \ (13)$ $0 < i < 2$, then $i = 1$

- Let $b \equiv 8^{2^{2-1-1}} \equiv 8 \ (13)$, so $b^2 \equiv 8^2 \equiv -1 \ (13)$
- Let $R = -4 \cdot 8 \equiv 7 \pmod{13}$, set $\underline{t \equiv (-1)(-1) = 1} \ (13)$ & $M = 1$

return $\boxed{R \equiv 7 \ (13)}$ $\boxed{\text{solution}}$

Cyclotomic Polynomials, Primes Congruent to 1 mod n

Cyclotomic Polynomials - just as we have primitive roots mod p, we can have primitive n^{th} roots of unity in the complex numbers. Recall that there are n distinct nth roots of unity - ie., solutions of $z^n = 1$, in the complex numbers. We can write them as $e^{2\pi ij/n}$ for $j = 0, 1, \ldots n-1$. They form a regular n-gon on the unit circle.

We say that z is a primitive nth root of unity if $z^d \neq 1$ for any d smaller than n. If we write $z = e^{2\pi ij/n}$, this is equivalent to saying $(j, n) = 1$. So there are $\phi(n)$ primitive nth roots of unity.

Eg. 4th roots of 1 are solutions of $z^4 - 1 = 0$, or $(z-1)(z+1)(z^2+1) = 0 \Rightarrow z = 1, -1 \pm i$

Now 1 is a primitive first root of unity, -1 is a primitive second root of unity, and $\pm i$ are primtiive fourth roots of unity. Notice that $\pm i$ are roots of the polynomial $z^2 + 1$. In general, define

$$\Phi_n(x) = \prod_{\substack{(j,n)=1 \\ 1 \leq j \leq n}} (x - e^{2\pi ij/n})$$

This is the $\boxed{n\text{th } \textbf{cyclotomic polynomial.}}$

We'll prove soon that $\Phi_n(x)$ is a polynomial with integer coefficients. Another fact is that it is **irreducible**, ie., cannot be factored into polynomials of smaller degree with integer coefficients (we won't prove this, however).

Anyway, here is how to compute $\Phi_n(x)$: take $x^n - 1$ and factor it. Remove all factors which divide $x^d - 1$ for some $d|n$ and less than n.

Eg. $\Phi_6(x)$. Start with $x^6 - 1 = (x^3-1)(x^3+1)$. Throw out $x^3 - 1$ since $3|6$ and $3 < 6$. $x^3 + 1 = (x+1)(x^2 - x + 1)$. Throw out $x + 1$ which divides $x^2 - 1$, since $2|6, 2 < 6$. We're left with $x^2 - x + 1$ and it must be $\Phi_6(x)$ since it has the right degree $2 = \boxed{\varphi(6)}$ (the nth cyclotomic polynomial has degree $\varphi(n)$, by definition).

If you write down the first few cyclotomic polynomials you'll notice that the coefficient seems to be 0 or ± 1. But in fact, $\Phi_{105}(x)$ has -2 as a coefficient, and the coefficients can be arbitrarily large if n is large enough.

These polynomials are very interesting and useful in number theory. For instance, we're going to use them to prove that given any n, there are infinitely many primes congruent to $1 \mod n$.

Eg. $\Phi_4(x) = x^2 + 1$ and the proof for primes $\equiv 1 \mod 4$ used $(2p_1 \ldots p_n)^2 + 1$

Proposition 45. *1.* $x^n - 1 = \prod_{d|n} \Phi_d(x)$

2. $\Phi_n(x)$ *has integer coefficients*

3. For $n \geq 2$, $\Phi_n(x)$ *is reciprocal; ie.,* $\Phi_n(\frac{1}{x}) \cdot x^{\varphi(n)} = \Phi_n(x)$ *(ie., coefficients are palindromic)*

Proof. **1.** is easy - we have

$$x^n - 1 = \prod_{1 \leq j \leq n} (x - e^{2\pi i j/n})$$

If $(j,n) = d$ then $e^{2\pi i j/n} = e^{2\pi i j'/n'}$ where $j' = \frac{j}{d}, n' = \frac{n}{d}$, and $(j', n') = 1$. $(x - e^{2\pi i j'/n'})$ is one of the factors of $\Phi_{n'}(x)$ and $n'|n$. Looking at all possible j, we recover all the factors of $\Phi_{n'}(x)$, for every n' dividing n, exactly once. So

$$x^n - 1 = \prod_{n'|n} \Phi_{n'}(x)$$

2. By induction. $\Phi_1(x) = x - 1$. Suppose true for $n < m$. Then

$$x^m - 1 = \prod_{d|m} \Phi_d(x) = \underbrace{\left(\prod_{\substack{d|m \\ d<m}} \Phi_d(x) \right)}_{\text{monic (by defn), integer coefficients (by ind. hypothesis)}} \cdot \Phi_m(x)$$

So $\Phi_m(x)$, obtained by dividing a polynomial with integer coefficients, by a monic polynomial with integer coefficients, also has integer coefficients. This completes the induction.

3. By induction. True for $n = 2$, since $\Phi_2(x) = x + 1$.

$$\Phi_2\left(\frac{1}{x}\right) x^{\varphi(2)} = \left(\frac{1}{x} + 1\right) x = x + 1 = \Phi_2(x)$$

Suppose true for $n < m$. If we plug in $\frac{1}{x}$ into

$$x^m - 1 = \prod_{d|m} \Phi_d(x)$$

$$\left(\frac{1}{x}\right)^m - 1 = \prod_{d|m} \Phi_d\left(\frac{1}{x}\right)$$

$$= \left(\prod_{\substack{1<d<m \\ d|m}} \Phi_d\left(\frac{1}{x}\right) \right) \cdot \Phi_m\left(\frac{1}{x}\right) \cdot \left(\frac{1}{x} - 1\right)$$

Multiply by $x^m = \sum_{x^d|m}\varphi(d) = \prod_{d|m} x^{\varphi(d)}$ - proved before - to get

$$1 - x^m = \left(\prod_{\substack{1<d<m \\ d|m}} \Phi_d\left(\frac{1}{x}\right) x^{\varphi(d)} \right) \cdot \Phi_m\left(\frac{1}{x}\right) x^{\varphi(m)} \cdot \left(\frac{1}{x} - 1\right) x$$

$$-(x^m - 1) = \left(\prod_{\substack{1<d<m \\ d|m}} \underbrace{\Phi_d(x)}_{\text{by ind hyp}} \right) \cdot \Phi_m\left(\frac{1}{x}\right) x^{\varphi(m)} \cdot (1 - x)$$

$$-\prod_{d|m} \Phi_d(x) = \left(\prod_{\substack{1<d<m \\ d|m}} \Phi_d(x) \right) \cdot \Phi_m\left(\frac{1}{x}\right) x^{\varphi(m)} \cdot (-\Phi_1(x))$$

Cancelling almost all the factors we get

$$\Phi_m(x) = \Phi_m\left(\frac{1}{x}\right) x^{\varphi(m)}$$

completing the induction. ∎

Lemma 46. *Let $p \nmid n$ and $m|n$ be a proper divisor of n (ie., $m \neq n$). Then $\Phi_n(x)$ and $x^m - 1$ cannot have a common root mod p.*

Proof. By contradiction. Suppose a is a common root mod p. Then $a^m \equiv 1 \mod p$ forces $(a, p) = 1$. Next,

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \overset{\text{has root } a}{\underline{\Phi_n(x)}} \prod_{\substack{d|n \\ d<n}} \Phi_d(x) \quad \text{has root } a$$

Notice that $x^m - 1 = \prod_{d|m} \Phi_d(x)$ has all its factors in the last product. So this shows $x^n - 1$ has a double root at a, ie., $(x^n - 1) \equiv (x - a)^2 f(x) \mod p$ for some $f(x)$. Then the derivative must also vanish at $a \mod p$, so $na^{n-1} \equiv 0 \mod p$.

But $p \nmid n$ and $p \nmid a$, a contradiction. (↯) ∎

Now, we're ready to prove the main theorem.

Theorem 47. *Let n be a positive integer. There are infinitely many primes congruent to $1 \mod n$.*

Proof. Suppose not, and let $p_1, p_2, \ldots p_N$ be all the primes congruent to $1 \mod n$. Choose some large number l and let $M = \Phi_n(lnp_1 \ldots p_N)$. Since $\Phi_n(x)$ is monic, if l is large enough, M will be > 1 and so divisible by some prime p, $p \nmid l$.

First, note that p cannot equal p_i for any i, since $\Phi_n(x)$ has constant term 1, and so p_i divides every term except the last of $\Phi_n(lnp_1 \ldots p_n) \Rightarrow$ it doesn't divide M. For the same reason we have $p \nmid n$. In fact, $(p, a) = 1$ where $a = lnp_1 \ldots p_N$.

Now $\Phi_n(a) \equiv 0 \mod p$ by definition, which means $a^n \equiv 1 \mod p$. By the lemma, we cannot have $a^m \equiv 1 \mod p$ for any $m|n, m < n$. So the order of a mod p is exactly n, which means that $n|p-1$ since $a^{p-1} \equiv 1 \mod p \Rightarrow p \equiv 1 \mod n$, exhibiting another prime which is $\equiv 1 \mod n$. Contradiction. ($\lightning$) ■

Note - we did not even need to assume that there's a single prime $\equiv 1 \mod n$; if $N = q$ take the empty product, ie., 1, and we end up looking at $\Phi_n(ln)$ for large l.

Arithmetic Functions

Today - Arithmetic functions, the Möbius function

(Definition) Arithmetic Function: An arithmetic function is a function $f : \mathbb{N} \to \mathbb{C}$

$n=10$

$\pi(n) = 4$

$d(n) = 4$

$\sigma(n) = 1+2+5+10 = 18$

~~$\sigma_2(10)$~~

$\sigma_2(10) = \sum_{d|10} d^2 = 1^2+2^2+5^2+10^2$
$= 130.$

$\omega(10) = 2$

$\Omega(10) = 2.$

Eg.

$\pi(n) =$ the number of primes $\leq n$
$d(n) =$ the number of positive divisors of n
$\sigma(n) =$ the sum of the positive divisors of n
$\sigma_k(n) =$ the sum of the kth powers of divisors of n
$\omega(n) =$ the number of distinct primes dividing n
$\Omega(n) =$ the number of primes dividing n counted with multiplicity
$\Gamma_k(n) = n^k$.

Eg.

$$\sigma(1) = 1$$
$$\sigma(2) = 1 + 2 = 3$$
$$\sigma(3) = 1 + 3 = 4$$
$$\sigma(6) = 1 + 2 + 3 + 6 = 12$$

# of primes $\leq n$

(Definition) Perfect Number: A **perfect number** n is one for which $\sigma(n) = 2n$ (eg., 6, 28, 496, etc.) $\sigma(6) = 1+2+3+6 = 2\cdot 6$; $\sigma(28) = 1+2+4+\cdots = 2\cdot 28$ | Σ positive divisors of n

$\boxed{\text{Big open conjecture: Every perfect number is even.}}$

Note: One can show that if n is an even perfect number, then $n = 2^{m-1}(2^m - 1)$ where $2^m - 1$ is a Mersenne prime (Euler)

(Definition) Multiplicative: If f is an arithmetic function such that whenever $(m, n) = 1$ then $f(mn) = f(m)f(n)$, we say f is **multiplicative**. If f satisfies the stronger property that $f(mn) = f(m)f(n)$ for all m, n (even if not coprime), we say f is **completely multiplicative**

Eg.

$$f(n) = \begin{cases} 1 & n = 1 \\ 0 & n \neq 1 \end{cases}$$

is completely multiplicative. It's sometimes called **1** (we'll see why soon).

Spring 2015 MAT 311 Number Theory

Homework 01, Due 02/12/2015 in class

Letao Zhang

February 4, 2015

Your solution to each problem should be complete, and be written in complete sentences where appropriate. Please show all work.

Textbook: *An introduction to the theory of numbers*, fifth Edition, by Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery

Problems:
Section 1.2:

- 1 (a) (c)
- 3 (a) (e)
- 4 (a)
- 12
- 16
- 23
- 35
- 43

Spring 2015 MAT 311 Number Theory

Homework 02, Due 02/17/2015 in class

Letao Zhang

February 4, 2015

Your solution to each problem should be complete, and be written in complete sentences where appropriate. Please show all work.

Textbook: *An introduction to the theory of numbers*, fifth Edition, by Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery

Problems of Section 1.3:

- 6
- 11
- 20
- 22 (6) (8) (12) (13) (15)
- 16
- 27

Spring 2015 MAT 311 Number Theory

Homework 03, Due 02/24/2015 in class

Letao Zhang

February 17, 2015

Your solution to each problem should be complete, and be written in complete sentences where appropriate. Please show all work.

Textbook: *An introduction to the theory of numbers*, fifth Edition, by Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery

Problems of Section 1.4:

- 4
- 10

Problems of Section 2.1

- 6
- 7
- 10

Spring 2015 MAT 311 Number Theory

Homework 04, Due 03/03/2015 in class

Letao Zhang

February 24, 2015

Your solution to each problem should be complete, and be written in complete sentences where appropriate. Please show all work.

Textbook: *An introduction to the theory of numbers*, fifth Edition, by Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery

Problems of Section 2.1

- 18
- 23
- 43

Problems of Section 2.2

- 5 (a), (d)
- 6
- 8

Problems of Section 2.3

- 1
- 7
- 8

Spring 2015 MAT 311 Number Theory

Homework 05, Due 03/24/2015 in class

Letao Zhang

March 13, 2015

Your solution to each problem should be complete, and be written in complete sentences where appropriate. Please show all work.

Textbook: *An introduction to the theory of numbers*, fifth Edition, by Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery

1. Solve (by hand) the congruence $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{143}$.
2. What are the last two digits of 2^{100} and of 3^{100} ?
3. Find the number of solutions of $x^2 \equiv x \pmod{m}$ for any positive integer m.
4. Let property P be : for any a coprime to n, we have $a^{n-1} \equiv 1 \pmod{n}$
   (a) Show that the number $n = 561$ satisfying P
   (b) Let n be a squarefree composite number satisfying P. Show that n has at least 3 prime factors
   (c) Write down a sufficient condition for $n = pqr$ (where p, q, r are primes) to satisfy property P.
5. Do there exist arbitrarily long sequences of consecutive integers, none of which are squarefree? (i.e. given any positive integer N, does there exist a sequence of integers $x, x+1, ..., x+N-1$ such that none of these is squarefree?) Prove your assertion.

Spring 2015 MAT 311 Number Theory

Homework 05, Due 03/31/2015 in class

Letao Zhang

March 26, 2015

Your solution to each problem should be complete, and be written in complete sentences where appropriate. Please show all work.

Textbook: *An introduction to the theory of numbers*, fifth Edition, by Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery

Section 2.8

- 1
- 3
- 8
- 12
- 13

Spring 2015 MAT 311 Number Theory

Homework 05, Due 04/07/2015 in class

Letao Zhang

April 2, 2015

Your solution to each problem should be complete, and be written in complete sentences where appropriate. Please show all work.

Textbook: *An introduction to the theory of numbers*, fifth Edition, by Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery

Section 3.1

- 7
- 10
- 15

Section 3.2

- 1
- 3
- 4 (a) (d) (e)

Practice MidtIerm Exam I

Spring 2015 MAT 311 Number Theory

April 8, 2015

- Last Name (print):
- First Name (print):
- ID number (print):

Instructions

- Please answer each question in the space provided, and write full solutions.
- Please show all work, explain your reasons, and state all theorems you appeal to.
- Unless otherwise marked, answers without justification will get little or no partial credit.
- Cross out anything the grader should ignore and circle or box the final answer.
- Do NOT round answers.
- No books, notes, or calculators are allowed while taking the exam.

Question 1: Determine if a is a quadraitic residue mod p

(a) $a = 2$, $p = 13$
(b) $a = 5$, $p = 23$
(c) $a = 10$, $p = 13$
(d) $a = 25$, $p = 23$

Answer:

(a) No
(b) no
(c) yes
(d) yes

Question 2: Determine the number of primitive roots mod m

(a) $m = 4$
(b) $m = 6$
(c) $m = 7$
(d) $m = 101$
(e) $m = 100$

Answer

(a) 1
(b) 1
(c) 2
(d) 40
(e) 0

Question 3: Find the order of a mod m, AND determine if a is primitive.

(a) $a = 2$, $m = 27$
(b) $a = 5$, $m = 27$
(c) $a = 10$, $m = 27$

Answer

(a) 18
(b) 18
(c) 3

Question 4: Can you find a number a such that every number in $\{1, 2, 3, \ldots, 16\}$ can be expressed as a power of a mod 17. Justify your answer. Answer: Yes.

Question 5: Find the order of $2, 4$ mod 31 answer:

(a) $ord_{31}(2) = 5$
(b) $ord_{31}(4) = 5$

Question 6: compute the following Legendre Symbol

(a) $\left(\frac{8}{7}\right)$
(b) $\left(\frac{8}{17}\right)$

answer

(a) 1
(b) 1

Question 7: Determine if the following quadratic residue mod p is solvable. If so, find all solutions mod p

(a) $2x^2 + 3x - 1 \equiv 0 \bmod 7$
(b) $x^2 - 5 \equiv 0 \bmod 13$

answer

(a) not solvable
(b) not solvable

Spring 2015 MAT 311 Number Theory

Homework 09, Due Thursday 04/30/2015 in class

Letao Zhang

April 23, 2015

Your solution to each problem should be complete, and be written in complete sentences where appropriate. Please show all work.

Textbook: *An introduction to the theory of numbers*, fifth Edition, by Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery

Section 3.3

- 1
- 3
- 5
- 9

Section 3.4

- 1 (c) (e)
- 4

Practice Final Exam

Spring 2015 MAT 311 Number Theory

May 5, 2015

- Last Name (print):
- First Name (print):
- ID number (print):

Instructions

- Please answer each question in the space provided, and write full solutions.
- Please show all work, explain your reasons, and state all theorems you appeal to.
- Unless otherwise marked, answers without justification will get little or no partial credit.
- Cross out anything the grader should ignore and circle or box the final answer.
- Do NOT round answers.
- No books, notes, or calculators are allowed while taking the exam.

Question 1: Find $(2100, 72)$ and $[2100, 72]$

Question 2: Find the value of the Legendre symbol

$$\left(\frac{73}{107}\right)$$

Question 3: Suppose $(a, b) = d$ and d is not a divisor of g. Prove that the equation $ax^2 + by^2 = g$ has no solutions with integers x, y.

Question 4: Suppose p is an odd prime and a is a quadratic residue of p. Prove that a is not a prmitive root of p

Question 5: Let $a = 2^7 \cdot 3^4 \cdot 11^9 \cdot 19$ and $b = 2^{17} \cdot 7^2 \cdot 11$

(a) find (a, b) and $[a, b]$

(b) Find the number of divisors of a

(c) Find $\phi(a)$ and $\phi(b)$

Question 6: Prove that for every integer n, $(n, 2n^2 + 1) = 1$

Question 7: True or False. Answer True or False.If it's false, please provide explanations, proofs or counterexamples.

(a) Every positive integer has a unique factorization into primes

(b) There are infinitely many primes p such that $p + 5$ is also a prime

(c) Every prime has a primitive root.

(d) For all positive integers m, n and all integers a, b the system of congruences has a solution x

$$x \equiv a \ (mod\ m)$$
$$x \equiv b \ (mod\ n)$$

(e) There are infinitely many primes p such that $p + 3$ is also a prime

(f) For all positive integers n and for all $b$such that $(b, n) = 1$, $ord_n b = \phi(n)$

Question 8: For each congruence, determine (with some explanation) if there are solutions or not.(x and y are integers)

(a) $8x \equiv 2 \pmod{180}$

(b) $x^7 \equiv 2 \pmod{47}$