

MAT 311: Number Theory Spring 2008

Solutions to HW2

1. Find all positive integers x such that $13 \mid x^2 + 1$
 $13 \mid x^2 + 1$ iff $x^2 + 1 \equiv 0 \pmod{13}$. Just by inspection (check for $x = 0, 1, 2, \dots, 6$, and use the fact that $x^2 \equiv (-x)^2$) we see that $x \equiv 5$ and hence $x \equiv -5 \equiv 8$ are the only solutions of this equation mod 13. Hence any such x is of the form $x = 5 + 13k$ or $x = 8 + 13k$. □

2. If p is a prime and $a^2 \equiv b^2 \pmod{p}$, show that $a \equiv b$ or $a \equiv -b \pmod{p}$.
 $a^2 \equiv b^2 \pmod{p} \Leftrightarrow a^2 - b^2 \equiv 0 \pmod{p} \Leftrightarrow p \mid a^2 - b^2 = (a - b)(a + b)$. But, since p is prime this implies $p \mid (a - b)$ or $p \mid (a + b)$; or in other words $a - b \equiv 0 \pmod{p}$ or $a + b \equiv 0 \pmod{p}$, as required. □

3. (a) Assume that $(a, m) = 1$. Show that there is an integer b such that $ab \equiv 1 \pmod{m}$. Show also that $(b, m) = 1$.
Since $(a, m) = 1$, there are integers x and y such that $ax + my = 1$. Take \pmod{m} of both sides: $ax \equiv 1 \pmod{m}$. So we can take $b := x$. Observe that we must have $(b, m) = 1$, because now $ab + my = 1$, so any common factor of b and m should be a factor of 1. Hence 1 is the only common divisor of b and m , i.e. $(b, m) = 1$. □
(b) Let r_1, \dots, r_s be a reduced system \pmod{p} . What is s ?
Since all numbers coprime to p are congruent either one of the numbers from 1 to $p - 1$, and since the any two of the are non-congruent we have $\{r_1, \dots, r_s\} = \{1, 2, \dots, p - 1\}$. Hence $s = p - 1$. □
(c) Show that $r_1 \cdots r_s \equiv -1 \pmod{p}$.
This is the celebrated Wilson's Theorem. You can prove it using (3ab) and (2) a as follows: Since $\{r_1, \dots, r_s\} = \{0, 1, \dots, p - 1\}$, what we need to show is in fact $1 \cdot p - 1 = (p - 1)! \equiv -1 \pmod{p}$. By (a), every number from 1 to $p - 1$ has a multiplicative inverse \pmod{p} , i.e. for every a in the set $\{0, 1, \dots, p - 1\}$ there is another number b in the same set (could be a itself) so that if we multiply them we get 1, that is, $ab \equiv 1 \pmod{p}$. Every such a will match with a *unique* $b \pmod{p}$. So the product $1 \cdot p - 1 \pmod{p}$ will cancel in pairs, EXCEPT for those a with self-inverse, i.e. for $a^2 \equiv 1$. But by (2), this holds iff $a \equiv 1$ or $a \equiv -1 \equiv p - 1 \pmod{p}$. So $1 \cdot 2 \cdots p - 2 \cdot p - 1 \equiv 1 \cdot p - 1 \equiv -1 \pmod{p}$. □

4. Show that if $(a, b) = 1$, then $(a + b, a^2 - ab + b^2) = 1$ or 3.
Note that $(a + b, a^2 - ab + b^2) = (a + b, a^2 - ab + b^2 - (a + b)^2) = (a + b, -3ab) = (a + b, 3ab)$. But on the other hand $(a, b) = 1 \Rightarrow (a, a + b) = 1$ and $(a + b, b) = 1 \Rightarrow (ab, a + b) = 1 \Rightarrow (a + b, 3ab) = 1$ or 3, as required. □

5. Using calculator find all solutions of $101x + 99y = 437$.
We use Euclid's algorithm to determine the solution set.

$$\begin{aligned} 101 &= 1 \cdot 99 + 2 \\ 99 &= 49 \cdot 2 + 1 \\ 2 &= 2 \cdot 1. \end{aligned}$$

So $1 = 99 - 49 \cdot 2 = 99 - 49 \cdot (101 - 99) = -49 \cdot 101 + 50 \cdot 99$. Thus the solutions are $x = -49 \cdot 437 + 99k = -21413 + 99k$,
 $y = 50 \cdot 437 - 101k = 21850 - 101k$, for $k \in \mathbb{Z}$. □