

Applied Algebra: Homework assignment 5
Due date: October 6

Fermat's and Euler's theorems:

1. Find

(a) $5^{20} \pmod{7}$ (b) $2^{16} \pmod{8}$ (c) $7^{1001} \pmod{11}$ (d) $6^{76} \pmod{13}$

2. Calculate $\varphi(32)$, $\varphi(21)$, $\varphi(120)$ and $\varphi(384)$.

Remark: if you already solved this problem in Homework 4, please do Problem 5 (about pirates) from Section 1.5 instead.

3. Show that, for every integer n , $n^{13} - n$ is divisible by 2, 3, 5, 7 and 13.

Public key codes:

4. A public key code has base 143 and exponent 103. It uses the following letter-to-number equivalents:

$$\begin{aligned} J = 1, \quad N = 2, \quad R = 3, \quad H = 4, \quad D = 5, \\ A = 6, \quad S = 7, \quad Y = 8, \quad T = 9, \quad O = 0. \end{aligned}$$

A message has been converted to numbers and broken into blocks. When coded using the above base and exponent the message sent is 10/03. Decode the message.

Identities modulo p :

5. (a) Prove the lazy student identities:

$$(a + b)^2 \equiv a^2 + b^2 \pmod{2},$$

and

$$(a_1 + a_2 + \dots + a_n)^2 \equiv a_1^2 + a_2^2 + \dots + a_n^2 \pmod{2}.$$

(b) Prove that

$$(a + b)^3 \equiv a^3 + b^3 \pmod{3}$$

(c) Is it true that

$$(a + b)^4 \equiv a^4 + b^4 \pmod{4}?$$

(d) Let p be a prime number. Prove the binomial theorem modulo p :

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Remark: The formula of part (d) is much simpler than the usual binomial formula. This is a manifestation of a more general principle: things become easier if one considers them modulo p . This principle is used very successfully in different branches of mathematics, and it is one of the reasons why we study congruence classes modulo p .

Bonus 6 (Euler's proof). Prove Fermat's Little Theorem using the following steps:

- (1) Prove that the polynomial $F(x) = x^p - x$ is divisible by p for any integer x if and only if all differences $F(x + 1) - F(x)$ are divisible by p for any integer x .
- (2) Prove that $F(x + 1) - F(x)$ is divisible by p using the binomial formula modulo p .