

# MATH 332 - ALGEBRA AND NUMBER THEORY : HOMEWORK 8

DUE FRIDAY, OCTOBER 20TH (NO LATER THAN 12PM)

## CHAPTER 5: QUADRATIC CONGRUENCES

**Problem 1.** Find the value of the following Legendre symbol:  $\left(\frac{4699}{4703}\right)$ . Note that 4703 is prime but 4699 is not!

*Proof.* The number 4699 factors as  $37 \cdot 127$ , and notice that they are both  $1 \pmod{4}$ , thus, by the properties of the Legendre symbol and quadratic reciprocity:

$$\left(\frac{4699}{4703}\right) = \left(\frac{37}{4703}\right) \cdot \left(\frac{127}{4703}\right) = \left(\frac{4703}{37}\right) \cdot \left(\frac{4703}{127}\right) = \left(\frac{4}{37}\right) \cdot \left(\frac{16}{127}\right) = 1.$$

□

**Problem 2.** Find all solutions of the following congruence:

$$x^2 - 7x + 47 \equiv 0 \pmod{35}.$$

In how many ways can you factor the polynomial  $x^2 - 7x + 47$  in  $\mathbb{Z}/35\mathbb{Z}$ ? Hint: there is more than one!

*Proof.* First, find all solutions modulo 5 and 7, separately. The discriminant is  $-139 \equiv 1 \pmod{5}$  and  $-139 \equiv 1 \pmod{7}$ . Thus:

$$\sqrt{\Delta} \equiv \pm 1 \pmod{5}, \quad \sqrt{\Delta} \equiv \pm 1 \pmod{7}$$

and

$$x \equiv \frac{2 \pm 1}{2} \equiv 4 \text{ or } 3 \pmod{5}, \quad x \equiv \frac{0 \pm 1}{2} \equiv 4 \text{ or } 3 \pmod{7}.$$

However, there are four possibilities modulo 35:

$$x \equiv 3(5), x \equiv 3(7) \implies x \equiv 3 \pmod{35}$$

$$x \equiv 4(5), x \equiv 4(7) \implies x \equiv 4 \pmod{35}$$

$$x \equiv 3(5), x \equiv 4(7) \implies x \equiv 18 \pmod{35}$$

$$x \equiv 4(5), x \equiv 3(7) \implies x \equiv 24 \pmod{35}$$

Hence,  $x \equiv 3, 4, 18, 24 \pmod{35}$  are all inequivalent roots modulo 35. Thus, if the polynomial  $x^2 - 7x + 47 \equiv x^2 - 7x + 12 \pmod{35}$  factors, it should factor as the product of two linear terms  $(x - a)(x - b)$  and  $a, b$  are roots such that  $ab \equiv 12 \pmod{35}$ . The only possibilities that work are:

$$(x - 3)(x - 4) = (x - 18)(x - 24).$$

□

**Problem 3.** Prove that RSA works and explain WHY it works (what theorem?), i.e. prove that with choices of  $p, q, n, d$  and  $e$  as above, if we form  $C \equiv M^e \pmod{n}$  then

$$M \equiv C^d \pmod{n}.$$

*Proof.* Notice that  $d$  and  $e$  are chosen so that  $d$  is the multiplicative inverse of  $e$  modulo  $\phi(n)$ . Hence,  $de = 1 + k\phi(n)$  for some  $k \in \mathbb{Z}$ . Now one simply calculates:

$$C^d \equiv M^{ed} \equiv M^{1+k\phi(n)} \equiv M \pmod{n}$$

because  $M^{\phi(n)} \equiv 1 \pmod{n}$  by Euler's Theorem. Notice that the message  $M$  needs to be relatively prime to  $n$  for this to work. But since  $n = pq$ , the gcd of  $n$  and  $M$  is 1 in most cases, so you only need to make sure to code your message in a way such that  $(M, n) = 1$ , which is easy to do.  $\square$

**Problem 4.** Suppose there is a public key  $n = 2911$  and  $e = 1867$  and you intercept an encrypted message:

0785 0976 1594 0481 1560 2128 0917.

- (1) Can you crack the code and decipher the message?
- (2) Another message is sent with public key  $n = 54298697624741$  and  $e = 1234567$ . Could you crack this code? How would you do it?

*Proof.* In order to crack an RSA code, the fundamental problem is to be able to factor  $n$ . In this case, this is easily accomplished because  $n$  is small enough. Indeed:  $n = 41 \cdot 71$ . Hence, we can calculate  $\phi(n) = \phi(41)\phi(71) = 40 \cdot 70 = 2800$ . Also, we can calculate  $d = e^{-1}$  modulo 2800:

$$d \equiv (1867)^{-1} \equiv 3 \pmod{2800}.$$

Now, we can start decoding the message, one block at a time:

$$(0785)^3 \equiv 1200 \pmod{2911}, \quad (0976)^3 \equiv 1907 \pmod{2911}, \dots$$

The full decoded message is:

1200 1907 0818 0022 0418 1412 0423

When we translate the code back into letters (remember  $00 = A$ ,  $01 = B$ , ...) we get:

MATHISAWESOMEX

Hence, the original message was “*Math is awesome*” (and a letter X was added at the end to finish a four digit block).  $\square$

## CHAPTER 6: PRIMITIVE ROOTS, ORDER AND INDEX

Solve the following problems from the book (p. 189): 1, 3, 4, 6, 7, 9.

**Solution of P-1.** (a) Notice that  $\phi(37) = 36$  and the divisors of 36 are 1, 2, 3, 4, 6, 9, 12, 18, 36, and the order of 34 must be one of these numbers. Also, notice that  $34 \equiv -3 \pmod{37}$ . Next, we calculate:

$$34^2 \equiv 9, \quad 34^3 \equiv -27 \equiv 10, \quad 34^4 \equiv -30 \equiv 7, \quad 34^6 \equiv 34^3 \cdot 34^3 \equiv 10 \cdot 10 \equiv 26$$

$$34^9 \equiv 34^6 \cdot 34^3 \equiv 260 \equiv 1 \pmod{37}$$

Therefore the order is 9.

- (b) Notice that if we put  $a = 2^{12}$ , then  $a^2 \equiv 2^{24}$  and  $a^3 = 2^{36} \equiv 1 \pmod{37}$ , by Fermat's Little Theorem. Hence, the order of  $a$  is a divisor of 3, and so  $\text{ord}(a) = 1$  or 3, and the order is 1 only if  $2^{12} \equiv 1 \pmod{37}$ . But  $2^{12} \equiv 26 \pmod{37}$ , hence its order is 3.

Another way of doing this is by realizing that 34 has order 9 and  $34^{9/3} \equiv 34^3 \equiv 10$  has order 3 (by Theorem 6.3ii). Then  $10^2 \equiv 26 \equiv 2^{12}$  must also have order 3.  $\square$

**Solution of P-3.** Notice that if  $m > 1$  then  $\phi(m) = m - 1$  if and only if  $m$  is prime (you can find a proof of this in Exercise 3-59 of the book). Moreover, for all  $m > 1$ ,  $\phi(m) \leq m - 1$ . If  $(a, m) = 1$  and the order of  $a$  is  $m - 1$ , since the order divides  $\phi(m)$  this implies that  $\phi(m) \geq m - 1$ , thus  $\phi(m) = m - 1$  and  $m$  must be prime.  $\square$

**Solution of P-4.** Notice that  $(4, 5) = 1$  and  $9 \cdot 10 \equiv 90 \equiv 8 \pmod{41}$ , thus  $\text{ord}(8) = \text{ord}(9) \cdot \text{ord}(10) = 20$ , by Theorem 6.4.  $\square$

**Solution of P-6.** The number 263 is prime, thus, if 5 is a primitive root, then the order of 5 is 262. Now,  $258 \equiv -5 \pmod{263}$ , and

$$258^t \equiv (-5)^t \equiv (-1)^t 5^t \equiv 263.$$

Notice that since 5 is a primitive root, the only times that  $5^t \equiv \pm 1$  are  $t = 161, 262$ . Thus,  $258^t \equiv 1$  happens for  $t = 161, 262$  as well ( $5^{161} \equiv -1$  by Euler's criterion). Hence, the order of  $-5$  is 161.  $\square$

**Solution of P-7.** For every prime  $p$ , there exists a primitive root, i.e. an element  $g$  of order  $p - 1$ . If there exists an element of order 4, then  $p - 1$  must be divisible by 4, i.e.  $p \equiv 1 \pmod{4}$ . By Theorem 6.3.ii, if  $p - 1$  is divisible by 4, then the element  $g^{(p-1)/4}$  has exact order 4. Thus, there is an element of order 4 only for the primes  $p \equiv 1 \pmod{4}$ .  $\square$

**Solution of P-9.** Since 2 is a primitive root and 101 is prime, 2 has order 100 and  $2^{100/5} \equiv 2^{20} \equiv 95 \pmod{101}$  has order 5. By Theorem 6.3i, the numbers 95,  $95^2 \equiv 36$ ,  $95^3 \equiv 87$ ,  $95^4 \equiv 84$  all have order 5. Finally, the equation

$$x^5 \equiv 1 \pmod{101}$$

has only 5 solutions modulo 101 by Lagrange's theorem, namely 1, 36, 84, 87 and 95, so the last four are all numbers of order 5.  $\square$