

MATH 332 - ALGEBRA AND NUMBER THEORY : HOMEWORK 8

DUE FRIDAY, OCTOBER 19TH (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!

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!

RSA: PUBLIC KEY CRYPTOGRAPHY

RSA is an example of public key cryptography. It is a widely used system, relying for its security on the difficulty of factoring a large number. The coding works as follows.

Suppose that there are two people, Alice and Bob, who want to communicate privately. First, we need a way to convert words into numbers. This can be done in many ways. One way is to assign a two digit number to each letter:

$$00 = A, \quad 01 = B, \quad 02 = C, \quad \dots, \quad 24 = Y, \quad 25 = Z.$$

The spaces between words are erased, and we make groups of two consecutive letters to form four digits numbers. For example, the message PUBLIC KEY CRYPTOGRAPHY would become:

$$1520 \ 0111 \ 0802 \ 1004 \ 2402 \ 1724 \ 1519 \ 1406 \ 1700 \ 1507 \ 2423$$

where we have added a dummy letter $X = 23$ at the end of the passage to fill out the final block. Now, we need a secure way to encrypt the message, which Bob will send to Alice.

Alice forms her public and private keys as follows:

- Chooses large primes p and q , then form $n = pq$.
- Chooses e coprime with $\phi(n) = (p - 1)(q - 1)$.
- Publishes (n, e) as her public key.
- Computes private key d such that $de \equiv 1 \pmod{\phi(n)}$.

For example, Alice may pick “large” primes $p = 43$, $q = 59$ and $n = 43 \cdot 59 = 2537$ as the modulus, and $e = 13$ as the exponent.

To encrypt a message M (where $M < n$) the user Bob forms $C \equiv M^e \pmod{n}$. To decrypt the message, Alice forms $P \equiv C^d \pmod{n}$. For example, the first block of our previous message $M = 1520$ would get encrypted as

$$C \equiv (M)^e \equiv (1520)^{13} \equiv 95 \pmod{2537}$$

which Bob would send over to Alice as 0095. The second block:

$$C \equiv (0111)^{13} \equiv 1648 \pmod{2537}$$

so Bob would send 1648 and so on. The complete encrypted message would be:

0095 1648 1410 1299 0811 2333 2132 0370 1185 1957 1084.

Now, to decrypt the message, since Alice knows p and q , she also knows $\phi(n) = \phi(43 \cdot 59) = 2436$. Using the Euclidean algorithm she easily finds $d = 937$ satisfies $de \equiv 1 \pmod{\phi(n)}$. Consequently, to decrypt the first block C sent over by Bob, she only needs to compute:

$$P \equiv C^{937} \equiv (0095)^{937} \equiv 1520 \pmod{2537}$$

and now Alice knows the first two letters of the message, i.e. P and U.

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

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

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?

Remark. *Currently, it takes several months of computing time (on the best computers available!) to factor numbers with 200 digits. In practice, the RSA codes used on the internet make use of values of n with 600 or 1200 digits, and the value of n is changed on a weekly basis.*

CHAPTER 6: PRIMITIVE ROOTS, ORDER AND INDEX

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