

## ELEMENTARY NUMBER THEORY

### MIDTERM 2

(1) Compute

(a)  $\phi(300)$ .

$$300 = 2^2 \cdot 3 \cdot 5^2, \text{ hence } \phi(300) = \phi(2^2) \cdot \phi(3) \cdot \phi(5^2) = 2 \cdot 2 \cdot 4 \cdot 5 = 80.$$

(b) the order of 2 mod 7.

We have  $2^2 \equiv 4 \pmod{7}$  and  $2^3 \equiv 1 \pmod{7}$ , hence the order of 2 mod 7 is equal to 3.

(c)  $88! \pmod{89}$ .

By Wilson's theorem, we have  $88! \equiv -1 \pmod{89}$ .

(2) Give the definition

(a) of a primitive root: an element  $g \in (\mathbb{Z}/m\mathbb{Z})^\times$  with order  $\phi(m)$ ; equivalently: an element whose powers give every element of  $(\mathbb{Z}/m\mathbb{Z})^\times$ .

(b) of the Legendre symbol.

We say that  $\left(\frac{a}{p}\right) = +1$  or  $= -1$  for odd primes  $p$  and integers  $a$  not divisible by  $p$  according as  $a$  is a square mod  $p$  or not.

(3) Explain why  $\phi(p^2) = p(p-1)$  for primes  $p$ .

The elements of  $(\mathbb{Z}/p^2\mathbb{Z})^\times$  are those from  $1, 2, \dots, p^2$  that are not divisible by  $p$ . Since there are  $p^2$  elements in the list, and since exactly the  $p$  elements  $p, 2p, \dots, p^2$  are divisible by  $p$ , we have  $\phi(p^2) = p^2 - p = p(p-1)$ .

(4) Compute  $2^{2000} \pmod{p}$  for the prime  $p = 4001$ .

By Euler's criterium, we have  $2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \pmod{p}$ . Using the second supplementary law and observing that  $4001 \equiv 1 \pmod{8}$  we see that  $2^{2000} \equiv 1 \pmod{p}$ .

(5) Describe how RSA works (how are private and public keys chosen, how is a message encrypted/decrypted, why does it work?).

See the notes. By "why it works" I meant the verification that  $c^d \equiv m \pmod{N}$ .

- (6) Compute  $24^{100} \pmod{99}$  (Hint: Chinese Remainder Theorem).

It is sufficient to compute  $x = 24^{100} \pmod{9}$  and  $\pmod{11}$ . Since  $3 \mid 24$ , we have  $9 \mid x$ , hence  $x \equiv 0 \pmod{9}$ . On the other hand,  $x = 24^{100} \equiv 2^{100} \equiv (2^{10})^{10} \equiv 1 \pmod{11}$  because of Fermat's little theorem. Solving the linear system  $x \equiv 0 \pmod{9}$  and  $x \equiv 1 \pmod{11}$  using Bezout or by trial and error gives  $x \equiv 45 \pmod{99}$ .

- (7) Compute  $\left(\frac{105}{1031}\right)$  (1031 is prime)

(a) using quadratic reciprocity for the Legendre symbol only;

$$\left(\frac{105}{1031}\right) = \left(\frac{3}{1031}\right)\left(\frac{5}{1031}\right)\left(\frac{7}{1031}\right) = (-1)^2\left(\frac{1031}{3}\right)\left(\frac{1031}{5}\right)\left(\frac{1031}{7}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{5}\right)\left(\frac{2}{7}\right) = (-1)(+1)(+1) = -1.$$

(b) using the Jacobi symbol.

$$\left(\frac{105}{1031}\right) = \left(\frac{1031}{105}\right) = \left(\frac{-19}{105}\right) = \left(\frac{19}{105}\right) = \left(\frac{105}{19}\right) = \left(\frac{-9}{19}\right) = \left(\frac{-1}{19}\right) = -1.$$

Here we have used the first supplementary law and the fact that  $9 = 3^2$  is a square.

- (8) Use Gauss's Lemma to compute  $\left(\frac{-3}{13}\right)$  for primes  $p = 6n + 1$ .

Originally I wanted you to compute  $\left(\frac{-3}{p}\right)$  for primes  $p = 6n + 1$  and then chose the simpler problem of computing  $\left(\frac{-3}{13}\right)$ , but I forgot to delete the condition "for primes  $p = 6n + 1$ ".

Here goes: take the half system  $\{1, 2, 3, 4, 5, 6\} \pmod{13}$ . Then

$$\begin{aligned} -3 \cdot 1 &\equiv -3, & -3 \cdot 4 &\equiv +1, \\ -3 \cdot 2 &\equiv -6, & -3 \cdot 5 &\equiv -2, \\ -3 \cdot 3 &\equiv +4, & -3 \cdot 6 &\equiv -5, \end{aligned}$$

where all the congruences are mod 13. Since there are 4 minus signs, we conclude that  $\left(\frac{-3}{13}\right) = (-1)^4 = +1$ .

- (9) Let  $p = a^4 + 4$  be a prime. Show that  $\left(\frac{a}{p}\right) = +1$ .

Clearly  $a$  must be odd. Since  $p = a^4 + 4 \equiv 2^2 \pmod{a}$  we see that  $\left(\frac{p}{a}\right) = +1$ . Next  $p \equiv 1 \pmod{4}$  since  $a^2 \equiv 1 \pmod{4}$  for odd values of  $a$ . By the reciprocity law we have  $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = 1$ .

A different solution is to observe that  $a^4 + 4 = (a^2 + 2)^2 - 4a^2 = (a^2 - 2a + 2)(a^2 + 2a + 2)$  is prime only if  $a = \pm 1$  (then  $p = 5$ ), and here  $\left(\frac{a}{p}\right) = +1$  can be verified directly.

- (10) Let  $a$  be a quadratic residue modulo  $p$ , where  $p$  is an odd prime. Show that  $a$  is not a primitive root mod  $p$ .

By definition,  $a$  is a primitive root if and only if it has order  $p - 1$  in  $(\mathbb{Z}/p\mathbb{Z})^\times$ . But since  $\left(\frac{a}{p}\right) = +1$ , we have  $a^{(p-1)/2} \equiv +1 \pmod{p}$  by Euler's criterium, hence the order of a quadratic residue divides  $\frac{p-1}{2}$ . Thus  $a$  is never a primitive root