

## 18.781 Problem Set 5 - Fall 2008

Due Tuesday, Oct. 14 at 1:00

1. Create your own public-key cryptosystem by picking two primes  $p_1, p_2$  (they don't need to be large!), setting  $n = p_1 p_2$ , and picking an exponent  $(d, \phi(n)) = 1$ . Illustrate the encryption and decryption procedure by picking a message  $m < n$ .

Let's take the primes 179 and 211. Then  $n = 37769$  and  $\phi(n) = 178 \cdot 210 = 37380$ . If we choose  $d = 29$ , then we can calculate the inverse of  $d \pmod{\phi(n)}$  to be 1289. Then we find that for the message 14, we have the encryption  $14^{29} \equiv 32057 \pmod{37769}$ . So our encrypted message is 32057. To decrypt this, we raise it to the 1289, and get back 14.

2. (Niven 2.5.3) If you are able to factor  $n = p_1 p_2$ , then it is easy to calculate  $\phi(n) = (p_1 - 1)(p_2 - 1)$ . Show that this also works in reverse: If you are given  $n = p_1 p_2$  and the value of  $\phi = (p_1 - 1)(p_2 - 1)$ , solve for  $p_1$  and  $p_2$ .

The clever method for solving this is to note that the quadratic polynomial with zeroes  $p_1, p_2$  is

$$f(x) = (x - p_1)(x - p_2) = x^2 - (p_1 + p_2)x + p_1 p_2 = x^2 - (n - \phi(n) + 1)x + n.$$

Now we just apply the quadratic formula to find the zeroes in terms of the coefficients:

$$p_1, p_2 = \frac{n - \phi(n) + 1 \pm \sqrt{(n - \phi(n) + 1)^2 - 4n}}{2}.$$

3. (Niven 2.5.5) If  $m$  is not squarefree, show that there exist  $a_1, a_2$  such that  $a_1 \not\equiv a_2 \pmod{m}$ , but  $a_1^k \equiv a_2^k \pmod{m}$  for  $k \geq 2$ .

Since  $m$  is not squarefree, we can find a  $p$  with  $p^2 | m$ . Then let  $a_1 = 0$  and  $a_2 = \frac{m}{p}$ . Then since  $0 < a_2 < m$ ,  $a_1 \not\equiv a_2 \pmod{m}$ . But the square of each is congruent to zero, since

$$a_2^2 = \frac{m^2}{p^2} = m \cdot \frac{m}{p^2} \equiv 0 \pmod{m}.$$

So every power 2 or greater for each is zero, so they are all congruent.

4. (Niven 2.8.2) Find a primitive root of 23.

We check the smallest residues.

$$2^{11} \equiv 1 \pmod{23},$$

$$3^{11} \equiv 1 \pmod{23},$$

$$5^{11} \equiv -1 \pmod{23}.$$

So the order of 5, that is, the smallest power that gives 1, is not 11. It is also not 2, since  $5^2 = 25 \equiv 2 \pmod{23}$ . We know the order must divide 22 by Fermat's theorem, so this only leaves 22, and 5 is a primitive root.

5. (Niven 2.8.3) How many primitive roots does 13 have?

Suppose we had a primitive root,  $g$ . Then the first 12 powers of  $g$  give the 12 nonzero residues modulo 13, so every primitive root must be expressible as a power of  $g$ . So for what  $i$  is  $g^i$  a primitive root modulo 13? Well, we need the first power of  $g^i$  that is equivalent to 1 to be the 12th. This means that

$$(g^i \text{ is a primitive root}) \iff [(g^i)^k \equiv 1 \pmod{13} \iff 12|k].$$

Now, since  $(g^i)^k = g^{ik} \equiv 1$  exactly when  $12|(ik)$ , we need  $12|(ik) \iff 12|k$ . This is just requiring  $(12, i) = 1$ . So the powers of  $g$  that are primitive roots are the powers coprime to 12, or  $g, g^5, g^7$ , and  $g^{11}$ . So 13 has four primitive roots. Since two is a primitive root, we get that the complete list of primitive roots is

$$2, 32 \equiv 6, 128 \equiv 11, \text{ and } 2048 \equiv 7.$$

Note that generalizing this argument gives the beautiful and goofy formula for the number of primitive roots mod  $n$ , assuming at least one exists:  $\phi(\phi(n))$ .

6. (Niven 2.8.9 & 2.8.15)

(a) Show that  $3^8 \equiv -1 \pmod{17}$ . Explain why this implies that 3 is a primitive root modulo 17.

$$3^8 \equiv 9^4 \equiv 81^2 \equiv 13^2 \equiv 169 \equiv -1 \pmod{17}.$$

Now, suppose 3 was not a primitive root modulo 17. Then 3 has order less than  $\phi(17) = 16$ . We also know that  $3^{16} \equiv 1 \pmod{17}$  by Fermat, so the order of 3 must divide 16. But the only divisors of 16 are smaller powers of 2, and they all divide 8. So if 3 is not a primitive root, its order must divide 8, and so  $3^8$  must give 1 mod 17. Since we just showed that  $3^8 \not\equiv 1$ , 3 must be a primitive root.

(b) Prove that if  $a$  has order  $h$  modulo  $p$ , and  $h$  is even, then  $a^{\frac{h}{2}} \equiv -1 \pmod{p}$ .

We are given that the order of  $a$  modulo  $p$  is  $h$ , and  $2|h$ . So let  $\frac{h}{2} = k$ . Then we have  $1 \leq k < h$  and

$$(a^k)^2 \equiv a^h \equiv 1 \pmod{p}.$$

From a previous problem, we know the only square roots of 1 are  $\pm 1$ , in a prime modulus. The inequality above gives that  $a^k$  cannot be 1, since  $k$  is positive and less than the order of  $a$ . This only leaves the value  $-1$ , so

$$a^{\frac{h}{2}} \equiv -1 \pmod{p}.$$

(Bonus) Prove that if  $p$  is prime, then

$$1^k + 2^k + \dots + (p-1)^k \equiv \begin{cases} 0 \pmod{p} & \text{if } (p-1) \nmid k, \\ -1 \pmod{p} & \text{if } (p-1) \mid k. \end{cases}$$