

## CS 170 Spring 2008 - Solutions to Homework #2

### Problem 1.20 (4 points each, 16 points total)

Note that there exists multiplicative inverse of  $a$  modulo  $N$  iff  $\gcd(a, N) = 1$ , i.e.  $a$  and  $N$  are relatively prime.

a) Find the inverse of 20 mod 79

$$\begin{aligned}79 &= 3 * 20 + 19 \\20 &= 1 * 19 + 1 \\19 &= 19 * 1 + 0\end{aligned}$$

Thus  $\gcd(79,20)=\gcd(20,19)=\gcd(19,1)=\gcd(1,0)=1$ , i.e. 20 and 79 are relatively prime. Find  $x, y$  such that  $20x + 79y = 1$  as following:

$$\begin{aligned}1 &= \underline{1} - \underline{0} \\&= \underline{1} - (\underline{19} - 19 * \underline{1}) = 20 * \underline{1} - \underline{19} \\&= 20 * (\underline{20} - \underline{19}) - \underline{19} = 20 * \underline{20} - 21 * \underline{19} \\&= 20 * \underline{20} - 21 * (\underline{79} - 3 * \underline{20}) = 83 * \underline{20} - 21 * \underline{79}.\end{aligned}$$

Therefore  $x = 83 = 4 \pmod{79}$  is the multiplicative inverse of 20 mod 79.

b) Find the inverse of 3 mod 62

$$\begin{aligned}62 &= 20 * 3 + 2 \\3 &= 1 * 2 + 1 \\2 &= 2 * 1 + 0\end{aligned}$$

Thus  $\gcd(62,3)=\gcd(3,3)=\gcd(2,1)=\gcd(1,0)=1$ , i.e. 3 and 62 are relatively prime. Find  $x, y$  such that  $3x + 62y = 1$  as following:

$$\begin{aligned}1 &= \underline{1} - \underline{0} \\&= \underline{1} - (\underline{2} - 2 * \underline{1}) = 3 * \underline{1} - \underline{2} \\&= 3 * (\underline{3} - 1 * \underline{2}) - \underline{2} = 3 * \underline{3} - 4 * \underline{2} \\&= 3 * \underline{3} - 4 * (\underline{62} - 20 * \underline{3}) = 83 * \underline{3} - 4 * \underline{62}.\end{aligned}$$

Therefore  $x = 83 = 21(\pmod{62})$  is the multiplicative inverse of 3 mod 62.

c) Find the inverse of 21 mod 91

$$\begin{aligned}\underline{91} &= 4 * \underline{21} + 7 \\ \underline{21} &= 3 * \underline{7} + 0\end{aligned}$$

Thus  $\gcd(91,21)=\gcd(21,7)=\gcd(3,0)=3$ , i.e. 3 and 62 are not relatively prime. Therefore, the inverse of 21 mod 91 does not exist.

d) Find the inverse of 5 mod 23

$$\begin{aligned}\underline{23} &= 4 * \underline{5} + 3 \\ \underline{5} &= 1 * \underline{3} + 2 \\ \underline{3} &= 1 * \underline{2} + 1 \\ \underline{2} &= 2 * \underline{1} + 0\end{aligned}$$

Thus  $\gcd(23,5)=\gcd(5,3)=\gcd(3,2)=\gcd(2,1)=1$ , i.e. 23 and 5 are relatively prime. Find  $x, y$  such that  $5x + 23y = 1$  as following:

$$\begin{aligned}1 &= \underline{1} - \underline{0} \\ &= \underline{1} - (\underline{2} - 2 * \underline{1}) = 3 * \underline{1} - \underline{2} \\ &= 3 * (\underline{3} - \underline{2}) - \underline{2} = 3 * \underline{3} - 4 * \underline{2} \\ &= 3 * \underline{3} - 4 * (\underline{5} - 1 * \underline{3}) = 7 * \underline{3} - 4 * \underline{5} \\ &= 7 * (\underline{23} - 4 * \underline{5}) - 4 * \underline{5} = -32 * \underline{5} + 7 * \underline{23}\end{aligned}$$

Therefore  $x = -32 = 14(\pmod{23})$  is the multiplicative inverse of 5 mod 23.

## Problem 1.27 (10 points)

For the choice of  $p = 17$ ,  $q = 23$ , and  $e = 3$ , we need to find  $d$  such that  $ed = 1 \pmod{(p-1)(q-1)}$ , i.e.  $3d = 1 \pmod{352}$ .

Run Euclid's extended GCD algorithm for the multiplicative inverse of 3 mod 352.

$$\begin{aligned}\underline{352} &= 117 * \underline{3} + 1 \\ \underline{3} &= 3 * \underline{1} + 0\end{aligned}$$

Thus  $\gcd(352,3)=\gcd(3,1)=1$ , i.e. 3 and 352 are relatively prime. Find  $x, y$  such that  $3x + 352y = 1$  as following:

$$1 = \underline{352} - 117 * \underline{3}$$

Therefore  $x = -117 = 235 \pmod{352}$ , we can set  $d = 235$ .

The encryption of message  $M^3 \pmod{N}$ . When  $M = 3$ ,  $41^3 = (41 * 41) * 41 = 117 * 41 = 105 \pmod{391}$ . Therefore,  $105 = 41^3 \pmod{391}$  is the encrypted message for  $M = 41$ .

### Problem 1.35 (5 points each, 20 points total)

(a) If a number  $1 \leq n < p$  to be its own inverse modulo  $p$ , we have  $n * n \equiv 1 \pmod{p}$  or equivalently,  $n^2 - 1 = (n - 1)(n + 1) \equiv 0 \pmod{p}$ . Solving for  $n$ , we get  $n = +1, p - 1$ . We observe that for all those values  $n$  is indeed its own inverse.

(b) Among the  $p - 1$  numbers, 1 and  $p - 1$  are their own inverses and the rest have a (different than themselves) unique inverse  $\pmod{p}$  (since  $p$  is prime). This implies a one-to-one mapping between each number  $a$  in  $\{2, \dots, p - 2\}$  and its inverse (some number in the same range not equal to  $a$ ). Thus, we can pair up the numbers in  $\{2, \dots, p - 2\}$  such that the product of each pair is  $1 \pmod{p}$ . Therefore,  $(p - 2)(p - 3) \dots 2 \equiv 1 \pmod{p} \Rightarrow (p - 1)! \equiv (p - 1) \equiv -1 \pmod{p}$ .

(c) Assume, towards contradiction that  $N$  is not a prime and also  $(N - 1)! \equiv -1 \pmod{N}$ . Then  $(N - 1)! = -1 + kN \Rightarrow 1 = -(N - 1)! + kN$  which implies that  $\gcd((N - 1)!, N) = 1$ . This is false if  $N$  not a prime since there exists some prime  $q < N$  that is a multiple of  $N$  which appears in the factorial product above.

(d) It is not clear how to calculate a factorial under modular arithmetic in polynomial time. The obvious method would involve  $\Theta(N) = \Theta(2^n)$  multiplications, where the size of the input is  $n = \Theta(\log N)$  bits. On the contrary, Fermat's test uses a divide-and-conquer method to calculate an exponential under modular arithmetic in  $O(n^3)$  time.

### Problem 1.41 (5 points each, 15 points total)

(a) Assume  $a \equiv x^2 \equiv y^2 \pmod{N}$  for  $1 \leq x, y < N$ . Then  $x^2 - y^2 \equiv 0 \pmod{N} \Rightarrow (x - y)(x + y) \equiv 0 \pmod{N}$ . This means either  $x - y \equiv 0 \pmod{N} \Rightarrow x = y$  since both  $0 < x, y < N$  or  $x + y \equiv 0 \pmod{N} \Rightarrow x = N - y$  since  $0 < x, y < N$ . Since  $N$  is an odd prime  $\geq 3$ , there are exactly two possible values:  $x$  and  $y = N - x$ .

(b) We will first show that for any two numbers  $x, y$  in the range  $\{1, 2, \dots, \frac{N-1}{2}\}$  we have  $x^2 \neq y^2 \pmod{N}$ . Assume towards contradiction that  $x^2 \equiv y^2 \Rightarrow (x - y)(x + y) \equiv 0$ . Since  $N$  is prime,  $x \neq y$  leaving  $x + y \equiv N$ . But both  $x, y \leq \frac{N-1}{2}$ , so  $x + y \leq N - 1$ , a contradiction.

Therefore, each of those  $\frac{N-1}{2}$  numbers defines a quadratic residue  $\pmod{N}$ . Also, from (a), the rest of the  $\frac{N-1}{2}$  numbers in the range  $\{\frac{N-1}{2} + 1, \dots, N - 1\}$  lead to the same residues. Adding 0 as a quadratic residue, we have exactly

$\frac{N+1}{2}$  of them.

(c) Take, say,  $N = 15$  and  $a = 1$  then the equation  $x^2 \equiv 1 \pmod{15}$  has solutions 1, 4, 14.

### Problem 1.42 (10 points)

Find  $d$  such that  $e * d \equiv 1 \pmod{p-1}$ .  $d$  exists since  $e$  and  $(p-1)$  are relatively prime. This operation takes  $O(n^3)$  bit operations using the extended Euclid's algorithm.

Consider  $m^{e*d} \pmod{p}$ .  $e * d$  can be replaced with  $1 + k(p-1)$  and we have  $m^{1+k(p-1)} \pmod{p}$ . This equals  $m * (m^{p-1})^k \pmod{p}$ , which equals  $m * 1 \pmod{p}$  due to Fermat's Little Theorem. Since  $m$  is less than  $p$ , we simply have the original  $m$ . So to decrypt, we simply raise  $m^e$  to the  $d$  power mod  $p$ , which takes  $O(n^3)$  bit operations.

The reason this is so easy to decrypt is that we can find  $d$  without having to factor the product of two large primes. Without the difficult one-way function of factoring  $N = p * q$ , this encryption scheme is trivial.