Ravi Dayabhai

6.042/18.062J Mathematics for Computer Science
Tom Leighton and Marten van Dijk

September 21, 2010

Problem Set 3

Problem 1. [16 points] Warmup Exercises

For the following parts, a correct numerical answer will only earn credit if accompanied by it's derivation. Show your work. (SEE LAST PAGE)

(a) [4 pts] Use the Pulverizer to find integers s and t such that $135s + 59t = \gcd(135, 59)$.

(b) [4 pts] Use the previous part to find the inverse of 59 modulo 135 in the range $\{1, \ldots, 134\}$.

RIGHT IDEA, DUMB MISTAKE!

(c) [4 pts] Use Euler's theorem to find the inverse of 17 modulo 31 in the range $\{1, \ldots, 30\}$.

(d) [4 pts] Find the remainder of 34^{82248} divided by 83. (*Hint: Euler's theorem.*)

Problem 2. [16 points]

Prove the following statements, assuming all numbers are positive integers.

(a) [4 pts] If $a \mid b$, then $\forall c$, $a \mid bc$ (SEE BACK.)

(b) [4 pts] If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$.

(c) [4 pts] $\forall c$, $a \mid b \Leftrightarrow ca \mid cb$

(d) [4 pts] $\gcd(ka, kb) = k \gcd(a, b)$

Problem 3. [20 points] In this problem, we will investigate numbers which are squares modulo a prime number p.

(a) [5 pts] An integer n is a square modulo p if there exists another integer x such that $n \equiv x^2 \pmod{p}$. Prove that $x^2 \equiv y^2 \pmod{p}$ if and only if $x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$. (*Hint:* $x^2 - y^2 = (x + y)(x - y)$) (SEE BACK)

(b) [5 pts] There is a simple test we can perform to see if a number n is a square modulo p. It states that

Theorem 1 (Euler's Criterion). *:*

(2) [A] **Thm.** $a|b \Rightarrow \forall c,\ a|bc$. $(a,b,c \in \mathbb{Z}^+)$

Proof $a|b \Rightarrow \exists k,\ b = k_1 a$. Thus, $a|bc \Rightarrow a|(k_1 a)c \Leftrightarrow (k_1 a)c = k_2 a$ for $k_2 = k_1 c$, which is an integer when multiplied by $a = bc$. □

(2) [B] **Thm.** $a|b \wedge a|c \Rightarrow a|sb+tc$ $(a,b,c,s,t \in \mathbb{Z}^+)$.

Proof. $sb+tc \stackrel{?}{=} k \cdot a$ for some $k \in \mathbb{Z}^+ \Leftrightarrow s(k_b a) + t(k_c a) \stackrel{?}{=} k \cdot a \Leftrightarrow$ $k_1 = sk_b + tk_c$, which is an integer when multiplied by $k = sb+tc$. □.

(2) [C] **Thm.** $a|b \Leftrightarrow ca|cb$, $\forall c$ $(a,b,c \in \mathbb{Z}^+)$

Proof: ① $a|b \Rightarrow ca|cb$ since $b = k_1 a \Rightarrow ca|cak_1$ which satisfies $\exists k_2\ cak_1 = k_2 a$ (i.e., $k_2 = ck_1$)

② $ca|cb \Rightarrow a|b$ since $cb = k_1 ca \Leftrightarrow b = k_1 a \Leftrightarrow a|b$.

Thus by ① & ②, the biconditional is proved. □

(2) [D] **Thm** $\gcd(ka, kb) = k \cdot \gcd(a,b)$ $(a,b \in \mathbb{Z}^+)$

Proof: $\gcd(a,b)$ can be expressed as $s^*a + t^*b$ where $s^*, t^* \in \mathbb{Z}$ that minimize $s^*a + t^*b > 0$. $k \cdot \gcd(a,b) = ks^*a + kt^*b$. We can show that $s^*(ka) + t^*(kb) = \gcd(ka, kb)$ by contradiction. $\gcd(ka, kb) = s'(ka) + t'(kb)$ where s', t' minimize $s'(ka) + t'(kb) > 0$. Factoring k out: $k(s'a + t'b)$, s', t' also minimize $s'a + t'b \Rightarrow s', t' = s^*, t^*$, but this contradicts $\gcd(ka, kb) \neq s^*(ka) + t^*(kb)$, Thus $\gcd(ka, kb) = \gcd(a,b) \cdot k$ □

(3) [A] **Proof.** To establish ① $x^2 \equiv y^2 \pmod p \Rightarrow x \equiv \pm y \pmod p$ we assume $p \mid x^2 - y^2 \Leftrightarrow p \mid (x-y)(x+y) \Rightarrow p \mid (x-y)$, which is definition of $x \equiv y \pmod p$. (This is sufficient to establish ①). Next, we need to show ② $x \equiv \pm y \pmod p \Rightarrow x^2 \equiv y^2 \pmod p$. To do this we must establish both of the following implications.

② CASE 1 $x \equiv y \pmod p \Rightarrow x^2 \equiv y^2 \pmod p$

∨

CASE 2 $x \equiv -y \pmod p \Rightarrow x^2 \equiv y^2 \pmod p$

CASE 1 We can assume $p \mid (x-y)$ by definition $\Rightarrow$ p divides any multiple of $(x-y)$, of which $(x-y)(x+y) = x^2 - y^2 \Rightarrow p \mid x^2 - y^2$ $\Leftrightarrow x^2 \equiv y^2 \pmod p$.

CASE 2 Similar reasoning as CASE 1. With both CASES established ① ∨ ② establishes the desired biconditional.

1. *If n is a square modulo p then $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*
2. *If n is not a square modulo p then $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.*

Prove the first part of Euler's Criterion. (*Hint: Use Fermat's theorem.*) (SEE BACK.)

(c) [10 pts] Assume that $p \equiv 3 \pmod 4$ and $n \equiv x^2 \pmod p$. Given n and p, find one possible value of x. (*Hint: Write p as $p = 4k+3$ and use Euler's Criterion. You might have to multiply two sides of an equation by n at one point.*) (SEE BACK)

Problem 4. [10 points] Prove that for any prime, p, and integer, $k \geq 1$,

$$\phi(p^k) = p^k - p^{k-1}, \qquad \text{(SEE BACK)}$$

where ϕ is Euler's function. (*Hint: Which numbers between 0 and $p^k - 1$ are divisible by p? How many are there?*)

Problem 5. [18 points] Here is a *very, very fun* game. We start with two distinct, positive integers written on a blackboard. Call them x and y. You and I now take turns. (I'll let you decide who goes first.) On each player's turn, he or she must write a new positive integer on the board that is a common divisor of two numbers that are already there. If a player can not play, then he or she loses.

For example, suppose that 12 and 15 are on the board initially. Your first play can be 3 or 1. Then I play 3 or 1, whichever one you did not play. Then you can not play, so you lose.

(a) [6 pts] Show that every number on the board at the end of the game is either x, y, or a positive divisor of $\gcd(x, y)$. (SEE BACK)

(b) [6 pts] Show that every positive divisor of $\gcd(x, y)$ is on the board at the end of the game. (SEE NEXT PAGE)

(c) [6 pts] Describe a strategy that lets you win this game every time. (SEE NEXT PAGE)

Problem 6. [20 points] In one of the previous problems, you calculated square roots of numbers modulo primes equivalent to 3 modulo 4. In this problem you will prove that there are an infinite number of such primes!

(a) [6 pts] As a warm-up, prove that there are an infinite number of prime numbers. (*Hint: Suppose that the set F of all prime numbers is finite, that is $F = \{p_1, p_2, \ldots, p_k\}$ and define $n = p_1 p_2 \ldots p_k + 1$.*) (SEE NEXT PAGE)

(b) [2 pts] Prove that if p is an odd prime, then $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. (SEE NEXT PAGE)

(c) [6 pts] Prove that if $n \equiv 3 \pmod 4$, then n has a prime factor $p \equiv 3 \pmod 4$. (SEE BACK OF NEXT PAGE)

③ [B] Proof: We assume $\exists x.\ n \equiv x^2 \pmod p$. By Fermat's little Theorem $x^{p-1} \equiv 1 \pmod p \iff x^{p-3}\,x^2 \equiv 1 \pmod p \iff n^{\frac{p-3}{2}} \cdot n \equiv 1 \pmod p$, $\iff n^{\frac{p-1}{2}} \equiv 1 \pmod p$. □

③ [C] A concrete example exists when $p=19$, $n=20$, $x=1$. Another example is when $p=7$, $n=872$, $x=8$. More generally, if n is square modulo p and $p \equiv 3 \pmod 4$, we can express $p = 4k+3 \Rightarrow n^{\frac{(4k+3)-1}{2}} \equiv 1 \bmod p$ (by Euler's criteria) $\Rightarrow n^{2k+1} - 1 = mp$ where m is a nonnegative integer. $n^{\frac{2(\frac{p-3}{4})+1}{}} - 1 \equiv mp \iff$

$n^{\frac{p-1}{2}} - 1 = mp \Rightarrow (n^{\frac{p-3}{2}})(n) = n(mp+1) \Rightarrow 1 \equiv x^2(mp+1) \bmod p$.

and because $(mp+1) \bmod p = 1$, $x^2 \equiv 1 \pmod p$ which by definition means $p \mid x^2 - 1 \iff 4k+3 \mid (x-1)(x+1) \Rightarrow 4k+3 \mid x-1$ or $4k+3 \mid x-1 \iff$ $\boxed{x = mp \pm 1}$ for some choice of nonnegative integer m.

$n^{2k+1} \equiv 1 \pmod p \Rightarrow n^{2k+2} \equiv n \pmod p \Rightarrow$

$(n^{(k+1)})^2 \equiv n \pmod p \Rightarrow (n^{k+1})^2 \equiv x^2 \pmod p \Rightarrow x$ could be $n^{k+1} = n^{\frac{p-3}{2}+1}$

④ Proof: Note that $\phi(p^k)$ counts the integers relatively prime to p^k on interval $[1, p^k]$. Those integers are those that are NOT multiples of P. We can count the integers that are multiples of p in $[1, p^k]$ by p^{k-1} (see Lemma and its proof below). Therefore $\phi(p^k)$ is the difference of count of integers in $[1, p^k] = p^k$ and p^{k-1},

Lemma: p^{k-1} counts integers divisible by prime p in $[1, p^k]$ for $k \geq 1$.

The set of integers divisible by p in $[1, p^k]$ (called S) $\iff$

$\{\forall j \in \mathbb{Z}^+ \mid 1 \leq jp \leq p^k\} \Rightarrow S = \{1, 2, \ldots, p^{k-1}\} \Rightarrow |S| = p^{k-1}$ □

⑤ [A] x, y are already on board, so we just need to show all other numbers are divisors of $\gcd(x,y)$. Numbers played by players are common divisors of $x, y \Rightarrow$ divisors of $\gcd(x,y)$ by Lemma below. □

Lemma. We will show by contradiction that all common divisors of $x, y \in \mathbb{Z}^+$ are divisors of $\gcd(x,y)$. Assume $\exists d \in \mathbb{Z}^+$ $d \mid x$ and $d \mid y$ and $d \nmid \gcd(x,y)$. Then $d \cdot \gcd(x,y) \mid x$ and $d \cdot \gcd(x,y) \mid y$, but $d \cdot \gcd(x,y) \geq \gcd(x,y)$ so $\gcd(x,y)$ isn't the greatest a common divisor or $d \cdot \gcd(x,y) \bmod d \neq 0$, but but are contradictions. □

(d) [8 pts] Let F be the set of all primes p such that $p \equiv 3 \pmod 4$. Prove by contradiction that F has an infinte number of primes. (SEE BACK)

(*Hint: Suppose that F is finite, that is $F = \{p_1, p_2, \ldots, p_k\}$ and define $n = 4p_1p_2 \ldots p_k - 1$. Prove that there exists a prime $p_i \in F$ such that $p_i | n$.*)

(5)[B]. The game terminates when all common divisors of $x, y \in \mathbb{Z}^+$ are written on the board. By Lemma in (5)[A], these are all divisors of $\gcd(x,y)$. These enumerate all divisors of $\gcd(x,y)$ because if there were a divisor of $\gcd(x,y)$ not on the board, the board would be missing a number (a contradiction) since a divisor of $\gcd(x,y)$ is a divisor of x and of y.

(5)[C]. Express $\gcd(x,y) = p_1^{k_1} p_2^{k_2} \cdots p_j^{k_j}$ for primes p_i such that all $p_i \leq \gcd(x,y)$ and $p_i \mid \gcd(x,y)$, i.e., prime factorization of $\gcd(x,y)$. By (5)[A] & (5)[B], the number of divisors of $\gcd(x,y) \Leftrightarrow$ number of divisors common to x, y. $\prod_{i=1}^{j} (k_i+1)$ counts the divisors of $\gcd(x,y) \Rightarrow$ number of divisors common to x, y. If $\prod_{i=1}^{j} (k_i+1)$ is odd, go first otherwise go second when x and $y \neq \gcd(x,y)$ Otherwise, $\left(\prod_{i=1}^{j} (k_i+1)\right) - 1$ determines number of common divisors, so go first if this is odd, otherwise go second.

(6)[A]. Proof: (by contradiction) Assume $F = \{p_1, p_2, \ldots p_k\}$ contains all primes and k is finite. Let $n = \left(\prod_{i=1}^{k} p_i\right) + 1$. $\forall p \in F$, $p \nmid n \Rightarrow n$ prime less than p divides $n \Rightarrow n$ is prime, which contradicts F containing all finitely many primes. ∎.

(4)[B]. Proof: p is odd prime $\Rightarrow (p > 2) \wedge (p \text{ is odd})$. Any odd o mod $p \equiv 1$ or 3 because $o = 2k+1$ for $k \in \mathbb{N}$ and $4 \nmid 2k$ (the definition of $o \equiv 1 \bmod 4$ when k is even. When k is odd, it can be represented as $k = 2k'+1$ so $4 \mid 2\underbrace{(2k'+1)}_{(\text{odd } k)} + 1 - 3 \Leftrightarrow 3 \bmod 4$. Thus any odd o mod 4 is either 1 or 3 (including odd primes). ∎

⑥C Proof: (by contradiction) Assume $n \equiv 3 \pmod 4$. Then, $\nexists p.((p \text{ is prime} \wedge p \mid n) \Rightarrow p \equiv 3 \pmod 4) \iff \forall p.(p \text{ is prime} \wedge p \mid n) \Rightarrow p \not\equiv 3 \pmod 4$. When n is prime (so n is odd prime and $n \equiv 3 \bmod p$), then $\exists p.((p \text{ is prime} \wedge p \mid n) \Rightarrow p \equiv 3 \pmod 4)$ because $p = n$ since the only prime factor of n is n. When n is composite, we can write its prime factorization as $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r}$. Since $\forall p\,(p \text{ is prime} \wedge p \mid n) \Rightarrow p \not\equiv 3 \pmod 4$, none of the prime factors of n (i.e., all $p_i^{k_i}$) are 3 mod 4, so they all must be $1 \pmod 4$ by ⑥B. However, $1 \equiv \prod_{i=1}^{r} p_i^{k_i}$ while $n \equiv 3 \pmod 4$. A contradiction is reached for all $n \equiv 3 \pmod 4$, therefore, $\exists p.((p \text{ is prime} \wedge p \mid n) \Rightarrow p \equiv 3 \pmod 4)$. □

⑥D. Proof. (by contradiction) Suppose F is finite (i.e., $F = \{p_1, \ldots, p_k\}$ for finite $k \in \mathbb{Z}^+$) and let $n = 4\left(\prod_{i=1}^{k} p_i\right) - 1$. We know $n \equiv 3 \pmod 4$ since by definition $4 \mid n-3 \iff 4 \mid \left(\left(\prod_{i=1}^{k} p_i - 1\right) - 3\right) \iff 4 \mid 4\left(\prod_{i=1}^{k} - 1\right)$. From ⑥A, $(\exists p_i \in F)\ p_i \mid n$. However, $\forall p \in F\ p \nmid n$. This is a contradiction, so, F cannot be finite. □

6.042J / 18.062J Mathematics for Computer Science
Fall 2010

① [A]

x	y	rem(x,y)	=	x − qy
135	59	17	=	135 − 2(59)
59	17	8	=	59 − 3(17) = 59 − 3(135 − 2(59)) = −3(135) + 7(59)
17	8	1	=	17 − 2(8) = (135 − 2(59)) − 2(−3(135) + 7(59))
(STOP ITERATION @) last nonzero →	1		=	7(135) − 16(59) ⇔ gcd(135, 59) ⇔ "135 is relatively prime with 59"
8	1	0		

① [B] We need to find $x : 59x \equiv 1 \pmod{135}$. From [A], $\exists s,t$ $135s + 59t = 1$ so $135s = (-1)(59t - 1)$ ⇒ both sides divisible by 135 ⇒ $t = x \in \{1, \ldots, 134\}$. Pulverizer gives s,t, therefore multiplicative inverse, x, is $\boxed{-16}$ ⇒ $135 - 16 = \boxed{119} \in \{1, \ldots, 134\}$.

④ [E] 17 and 31 are relatively prime (and both prime, for that matter). By Euler's Theorem, $(17^{\phi(31)-1})17 \equiv 1 \pmod{31}$. $\phi(31) = 30$ since all positive integers < prime p are relatively prime to p. Therefore 17^{29} is a multiplicative inverse of 17 mod 31. $17^{29} \bmod 31 \equiv \boxed{11}$ because $17^{27} \equiv (10)^{14} \cdot 17 \pmod{31} \Leftrightarrow (7^7)(17) \bmod 31 \Leftrightarrow (18^3)(7)(17) \bmod 31 \Leftrightarrow (14)(18)(26) \bmod 31 \Leftrightarrow (18)(27) \bmod 31$.

④ [D]. By Euler's Theorem, $(34^{\phi(83)-1})34 \equiv 1 \bmod 83$ ⇒ the multiplicative inverse of 34 mod 83 is 34^{81} we can express 34^{82248} as $34^{(82\lfloor 82248/82 \rfloor + (82248 \bmod 82))} = 34^{(82248 \bmod 82)}$ mod 83. This, $34^{82248} = 34^2 \equiv \boxed{77 \pmod{85}}$.