Tom Leighton and Marten van Dijk

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.

(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 $\{1, \ldots, 134\}$.

(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 $\forall c$, $a \mid bc$

(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:* $x^2 - y^2 = (x + y)(x - y)$)

(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)**.** *:*

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.*)

(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.*)

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

$$\phi(p^k) = p^k - p^{k-1},$$

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 $\gcd(x, y)$.

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

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

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 $n = p_1 p_2 \ldots p_k + 1$.*)

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

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

(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.

(*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 $p_i | n$.*)

6.042J / 18.062J Mathematics for Computer Science
Fall 2010