Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 6
October 16, 2006
Due: NA

Problem Set 3 Number Theory Supplementary Exercises

Some supplementary number theory exercises that you do not need to hand in. Try to do them on your own. Ask the TAs if you have any questions.

Problem 3-1. Prove these statements:

(a) If $k|mn$ but $GCD(m,k) = 1$ then $k|n$.

(b) If $m > n$ then $GCD(m,n) = GCD(m-n,n)$.

(c) $GCD(m,n)$ is a linear combination of m and n.

(d) 1 can be written as an integer linear combination of 18 and 31.

(e) If $GCD(a,m) = 1$ and $GCD(a,n) = 1$ then $GCD(a,mn) = 1$.

(f) For all integers a and b and all positive numbers n, if $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.

(g) For all integers a, b, c, and all positive numbers n, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

(h) If $a \equiv b \pmod{n}$ then for all integers $c, c + a \equiv c + b \pmod{n}$.

(i) If $a \equiv b \pmod{n}$ then for all integers $c, ac \equiv bc \pmod{n}$.

(j) If $a \equiv b \pmod{n}$ then for all positive integers $c, a^c \equiv b^c \pmod{n}$.

(k) If a and n are relatively prime, then there is an integer a' such that $aa' \equiv 1 \pmod{n}$.

(l) If a and n are not relatively prime, then a has no multiplicative inverse modulo n.

(m) If $ab \equiv ac \pmod{n}$ and a has an inverse modulo n, then $b \equiv c \pmod{n}$, but this is not necessarily true if a does not have an inverse.

(n) If p is prime and $a \not\equiv 0 \pmod{p}$, then $(a)(2a)\ldots((p-1)a) \equiv (p-1)! \pmod{p}$.

(o) If $GCD(a,p) = 1$ where p is prime, then the order of a modulo p divides $p - 1$.

(p) If p and q are distinct primes, then if $GCD(a,pq) = 1$ then $a^{\phi(pq)} \equiv 1 \pmod{pq}$.

(q) If g is a generator modulo p and $GCD(a,p) = 1$, then there is an x such that $g^x \equiv a \pmod{p}$.

Problem 3-2. Some Multiple choice problems

(a) Which of the following statements is true:

a. A number is rational if and only if its square is rational.
b. An integer n is odd if and only if $n^2 + 2n$ is odd.
c. A number is irrational if and only if its square is irrational.
d. A number n is odd if and only if $n(n+1)$ is even
e. At least one of two numbers x and y is irrational if and only if the product xy is irrational.

(b) Which of the following statements is true:

a. A number k divides the sum of three consecutive integers $n, n+1$, and $n+2$ if and only if it divides the middle integer $n+1$.
b. An integer n is divisible by 6 if and only if it is divisible by 3.
c. For all integers a, b, and $c, a|bc$ if and only if $a|b$ and $a|c$.
d. For all integers a, b, and $c, a|(b+c)$ if and only if $a|b$ and $a|c$.
e. If r and s are integers, then $r|s$ if and only if $r^2|s^2$.

(c) For all $N \geq 0$, if $N = k(k+1)(k+2)$ is the product of three consecutive non-negative integers then for some integer $s > k, N$ is divisible by a number of the form

a. $s^2 - 1$
b. $s^2 - 2$
c. s^2
d. $s^2 + 1$
e. $s^2 + 2$

(d) The Euclidean Algorithm is used to produce a sequence $X_1 > X_2 > \ldots > X_{k-1} > X_k = 0$ of positive integers where each $X_t, 2 < t \leq k$, is the remainder gotten by dividing X_{t-2} by X_{t-1}. If $X_{k-1} = 45$ then the set of all (positive) common divisors of X_1 and X_2 is

a. 1, 3, 5
b. 1, 3, 5, 9, 15,
c. 1, 9, 15, 45
d. 1, 3, 5, 15
e. 1, 3, 5, 9, 15, 45

(e) Let L be the least common multiple of 175 and 105. Among all of the common divisors $x > 1$ of 175 and 105, let D be the smallest. Which is correct of the following:

a. $D = 5$ and $L = 1050$
b. $D = 5$ and $L = 35$
c. $D = 7$ and $L = 525$
d. $D = 5$ and $L = 525$
e. $D = 7$ and $L = 1050$

(f) The Euclidean Algorithm is used to produce a sequence $X_1 > X_2 > X_3 > X_4 > X_5 = 0$ of positive integers where $X_t = q_{t+1}X_{t+1} + X_{t+2}, t = 1, 2, 3$. The quotients are $q_2 = 3, q_3 = 2$, and $q_4 = 2$. Which of the following is correct?

a. $gcd(X_1, X_2) = -2X_1 + 6X_2$
b. $gcd(X_1, X_2) = -2X_1 - 6X_2$
c. $gcd(X_1, X_2) = -2X_1 - 7X_2$
d. $gcd(X_1, X_2) = 2X_1 + 7X_2$
e. $gcd(X_1, X_2) = -2X_1 + 7X_2$