# CS 70, Fall 2000
# Midterm 2
# Papadimtriou/Russell/Sinclair

**Problem #1**
**(20 pts.) Extended GCD**
For each of the following equations, find a pair of integers $x$ and $y$ that satisfies that equation or prove that no such pair exists.
[*Note*: these are *not* simultaneous equations.]

(a) (5 pts) $13x+ 21y = 1$

(b) (5 pts) $13x+ 21y = 2$

(c) (5 pts) $33x+ 21y = 1$

(d) (5 pts) $33x+ 21y = 3$

**Problem #2**
**(20+5 pts.) Perfect Squares**
Let $p$ be a prime greater than 2. An integer $y$ is called a *perfect square* modulo $p$ if $y = x^2 \bmod p$ for some integer $x$; $x$ is called a *square root* of $y$ modulo $p$.

(a) (6 pts) Which among the integers 0,1,...,10 are perfect squares modulo 11?

(b) (8 pts) Prove rigorously that each integer $y$, where $0 < y < p$, has either zero or two square roots modulo $p$.
[*Hint*: Suppose $w$ and $x$ are square roots of $y$; what can you deduce about the relationship between them?]

(c) (6 pts) Using the result in (b), prove that there are exactly $(p+1)/2$ perfect squares modulo $p$.

(d) (5 pts, extra credit) Prove that there are at least $p/3$ perfect cubes modulo $p$.

**Problem #3**
**(20 pts.) RSA**
Your public key is $p*q = 33$, with an exponent $e$ that is either 5 or 7.

(a) (4 pts) Which of 5 and 7 should be your public exponent, $e$? Why?

(b) (4 pts) What is your private key?

(c) (6 pts) How would you encrypt the message $m = 2$?

(d) (6 pts) How would you sign the same message?

**Problem #4**
**(20 pts.) Polynomials**

(a) (5 pts) A function *f*(*x*) on *GFp* returns a value in *GFp* given any input *x*, where *x* is an element of *GFp*. Two functions *f* and *g* are distinct if there is some value *x* for which *f*(*x*) ≠ g(*x*). How many distinct functions are there on *GFp*?

(b) (5 pts) Any polynomial on *GFp* can be written as

*q*(*x*) = (*Ap*-1)*x^(*p*-1) + (*Ap*-2)*x^(*p*-2) + ... + *A*0

where the coefficients *Ap*-1,...,*A*0 must also be in *GFp* . Two such polynomials are *apparently distinct* if they have different coefficients. How many apparently distinct polynomials are there on *GFp* ?

(c) (5 pts) Prove that if two polynomials q(*x*) and r(*x*) on *GFp* are apparently distinct then they are distinct functions.

(d) (5 pts) Hence show that every function on *GFp* is also a polynomial on *GFp*. (Note: Lagrange interpolation is a constructive proof of this fact, but we are not asking for a constructive proof in this problem.)

**Problem #5**
**(20+5 pts.) Probability spaces**

Each of the 50 states has two US senators. A committee of 20 senators is chosen uniformly at random from among all 100 senators. Answer the following questions, justifying each answer carefully:

(a) (6 pts) What is the sample space, and what is the probability of each sample point? [Your answer may contain binomial coefficients of the form $\binom{x}{y}$.]

(b) (6 pts) Let *CC* by the event that the committee includes both of the senators from California. What is the probability of *CC*?
[Your answer should be expressed as a rational number in reduced form.]

(c) (6 pts) Let *W* be the event that the committee contains at least one senator from Wyoming. What is the conditional probability of *CC* given *W*?
[Your answer should be expressed as a rational number in reduced form.]

(d) (2 pts) Are *CC* and *W* independent events? Remember to justify your answer.
(e) (5 pts, extra credit) What is the probability that at least one state has two members in the committee?
[Your answer may contain binomial coefficients of the form $\binom{x}{y}$.]

---