PMAT 527/627 Practice Midterm

October 13, 2012

1 Material

The following is a list of topics that may be on the exam.

1. Background: modular arithmetic, basic properties of divisibility, Euler's theorem, the definition of the ϕ function, computing $\phi(n)$ given a factorization of n, Lagrange's theorem, properties of cyclic groups.
2. Algorithmic complexity $(O(f), \Theta(f), \Omega(f), f \sim g)$
3. Exponentiation via repeated squaring.
4. The Euclidean algorithm, both basic and extended versions. The estimates on the number of divisions required and the overall running time. Executing the algorithm with actual numbers.
5. Arithmetic in $\mathbb{Z}/n\mathbb{Z}$, including computing inverses.
6. The Chinese remainder theorem: the consequences of $\theta\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ being an isomorphism of rings as well as the ability to recover a residue modulo n from a collection of residues modulo $n_1, \ldots, n_k$.
7. Primitive roots and multiplicative orders. Executing the algorithms to compute the multiplicative order of an element modulo n and to find a generator modulo p.
8. Legendre and Jacobi symbols. The ability to compute Jacobi symbols using quadratic reciprocity as well as $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.
9. Square roots modulo p. Executing the algorithms to compute the square root of an integer a modulo p.
10. Randomized algorithms. The difference between Atlantic City, Monte Carlo and Las Vegas algorithms. Definitions of expected running time and worst case running time.
11. Fermat's little theorem and Fermat test. Properties of Carmichael numbers and their frequency.
12. Miller-Rabin test. Executing the algorithm given a candidate prime p. Likelihood of failure and why Carmichael numbers are important in the superiority of the Miller-Rabin test to the Fermat test.
13. Lucas sequences (U_j and V_j). The divisibility of $U_{p\pm1}$ by p. The ability to compute U_j and V_j using a binary Lucas chain.
14. The Frobenius automorphism F of a finite field $\mathbb{F}_q$. What it means for an element $x \in \mathbb{F}_q$ to be fixed by F. How F acts on the roots of a polynomial $f(x)$ defining $\mathbb{F}_q$. For quadratic $f(x) = x^2 - ax + b$ why the Legendre symbol $\left(\frac{\Delta}{p}\right)$ controls the properties of $\mathbb{F}_p[x]/(f(x))$.
15. The Lucas-Lehmer test. Executing the test to determine if some $2^p - 1$ is prime.

2 Practice Problems

1. Let f and g be eventually positive functions. Prove that
   (a) $f = \Theta(g)$ if and only if $\log f = \log g + O(1)$.
   (b) $f \sim g$ if and only if $\log f = \log g + o(1)$.
2. Describe a process for computing $5^{261} \pmod{1009}$ that uses fewer than 12 arithmetic operations in $\mathbb{Z}/1009\mathbb{Z}$. You do not need to actually compute the result.
3. Find a solution to the following system of equations:
$$\begin{aligned} 20x &\equiv 8 \pmod{52} \\ 9x &\equiv 2 \pmod{35} \end{aligned}$$
4. Find a multiplicative generator modulo 41 (Hint: Jacobi symbols can help).
5. Show that for $p \equiv 1 \pmod 4$, the sum of the quadratic residues a with $0 < a < p$ is $p(p-1)/4$.
6. Prove that a primitive root for an odd prime p is a quadratic non-residue.
7. Prove that every composite Fermat number $2^{2^n} + 1$ is a Fermat pseudoprime base 2.
8. Show that for $p > 3$ prime,
$$\left(\frac{-3}{p}\right) = (-1)^{\frac{(p-1) \mod 6}{4}}.$$
9. Let a be an integer and suppose that the polynomial $x^3 - a$ is irreducible in $\mathbb{F}_p[x]$. Prove that $p \equiv 1 \pmod 6$. (Bonus: How is this related to the previous problem?)
10. Is the Fermat test for primality an Atlantic City, Monte Carlo or Las Vegas algorithm?
11. Run through the algorithm for computing the square root of $2 \pmod 7$ that uses arithmetic in $\mathbb{F}_{49}$.

3 Timed Problems

I've tried to estimate the length of the exam. The following questions should take you 50 minutes.

1. For each pair $f(n)$ and $g(n)$ indicate whether $f = O(g)$, $f = \Omega(g)$ and $f = o(g)$. You do not need to justify your answer.

f	g	$f = O(g)$	$f = \Omega(g)$	$f = o(g)$
$n^2 \log(n) + n$	$n \log(n)^2 - n$			
$2(n+1)^5$	$3(n-1)^5$			
$2^n + n^5$	$e^n + n^4$			
$n \log(n) + 1$	$n \log(n) + n$			

2. (a) Use the extended Euclidean algorithm to find integers a and b with $1001a + 92b = 1$.

(b) What is the inverse of 92 modulo 1001? What is the inverse of 1001 modulo 92?

(c) Note that $1001 = 11 \cdot 91$. Find the inverse of 92 modulo 91 and 11 and use the Chinese remainder theorem to reconstruct the inverse modulo 1001.

3. Use the Lucas-Lehmer test to prove that $31 = 2^5 - 1$ is prime.

4. Determine if $6601 = 7 \cdot 23 \cdot 41$ is a Carmichael number.

5. Consider the sequence U_j defined by

$$U_0 = 0$$
$$U_1 = 1$$
$$U_j = 6U_{j-1} - U_{j-2} \text{ for } j \geq 2.$$

(a) Describe the process for computing $U_{102} \pmod{101}$ using a Lucas binary chain. You do not actually need to compute it numerically.

(b) Without running through the computation of the Lucas chain, predict the value of $U_{102} \pmod{101}$. Justify your answer.