MATH 116

Last Midterm Examination

April Fools' Day, 2010

11:10AM–12:30 PM, 3109 Etcheverry Hall

Please put away all books, calculators, and other portable electronic devices—anything with an ON/OFF switch. You may refer to a single 2-sided sheet of notes. For numerical questions, *show your work* but do not worry about simplifying answers. For proofs, write your arguments in complete sentences that explain what you are doing. Remember that your paper becomes your only representative after the exam is over.

All five problems were worth 6 points. The mean was 14.1, the median 14. The standard deviation was 9.2.

1. Let $F = \mathbf{F}_{p^n}$, where p is an odd prime number and n a positive integer.

a. Show that $(a+b)^p = a^p + b^p$ for all $a, b \in F$.

The binomial theorem yields $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$. We need to see that the intermediate terms $\binom{p}{i} a^i b^{p-i}$ with $1 \le i \le p-1$ are all 0. In $\mathbf{F}$, $p = 0$, and it is enough to know that $\binom{p}{i}$ is a multiple of p. We have $p! = \binom{p}{i} i!(p-i)!$. Here, p divides the left-hand side of the equation, so it divides one of the three integers $\binom{p}{i}$, $i!$, $(p-i)!$. It doesn't divide the second or three of these integers, so it must divide the first.

b. Let $\zeta \in F^*$ be a qth root of 1, where q is an odd prime number different from p. Set

$$G = \sum_{i=1}^{q-1} \left(\frac{i}{q}\right) \zeta^i.$$

Prove that we have $G^p = \left(\frac{p}{q}\right) G$.

This is a computation that we did in class. By part (a), G^p is the sum of the pth powers of the terms defining G. Since the Legendre symbols $\left(\frac{i}{q}\right)$ are ± 1, they're their own pth powers. Hence $G^p = \sum_{i=1}^{q-1} \left(\frac{i}{q}\right) \zeta^{pi}$. Setting $j = pi$, we have $G^p = \sum_{j=1}^{q-1} \left(\frac{jp^{-1}}{q}\right) \zeta^j$. Since $\left(\frac{jp^{-1}}{q}\right) = \left(\frac{p}{q}\right)\left(\frac{j}{q}\right)$, the desired result follows.

2. a. A fair coin is tossed $2n$ times. What is the probability that exactly n heads come up? Write this probability as a rational number in lowest terms when $n = 6$.

For my dime, the probability is $\binom{2n}{n}/2^n$. When $n = 6$, we get $231/1024 = 0.2255859375$ for this expression.

b. Determine whether 1234 is a square modulo $12345 = 3 \cdot 5 \cdot 823$.

The number 1234 is the product of 2 and 617. Because $12345 \equiv 1 \bmod 8$, we have $\left(\frac{2}{12345}\right) = 1$. Hence $\left(\frac{1234}{12345}\right) = \left(\frac{617}{12345}\right)$, which may be rewritten $\left(\frac{12345}{617}\right)$ by quadratic reciprocity because $12345 \equiv 1 \bmod 4$.

Since $12345 \equiv 5 \bmod 1234$, we get $12345 \equiv 5 \bmod 617$. Hence $\left(\frac{1234}{12345}\right) = \left(\frac{5}{617}\right)$. Again by quadratic reciprocity, the latter symbol may be rewritten $\left(\frac{617}{5}\right)$. Since $617 \equiv 2 \bmod 5$ and 2 is not a square mod 5, we get finally that $\left(\frac{1234}{12345}\right)$ is -1. Thus 1234 is *not* a square mod 12345. Of course, if it turned out that we have $\left(\frac{1234}{12345}\right) = +1$, we wouldn't be able to conclude directly that 1234 is a square: we'd have to look separately mod 3, 5 and 823. Notice, however, that 1234 is 1 mod 3 and thus a square mod 3. Similarly, it's 4 mod 5 and thus a square mod 5. Hence the problem is equivalent to deciding whether 1234 is a square mod the prime 823. We have $1234 \equiv 411 = 3 \cdot 137 \bmod 823$, and one can certainly do the problem this way without referring to Jacobi symbols.

3. Let p be the prime number 251; note that $p - 1 = 2 \cdot 5^3$. Suppose that g is the primitive root 6 mod p, and that $h = 7 \bmod p$. Let x be the discrete logarithm $\log_g(h)$.

a. Use the Legendre symbol to find x mod 2.

The point is that x is a number mod 250 that we can determine by doing three computations mod 5 and one computation mod 2. (This is the Pohlig–Hellman business.) The question of whether or not x is even is the question of whether h is a square mod p. Now $\left(\frac{7}{251}\right) = -\left(\frac{251}{7}\right) = -\left(\frac{6}{7}\right) = -(-1) = +1$. Hence x is even.

b. Using the equation $g^{150} = h^{50}$ and the result of part (**a**), find the value of x mod 10.

The given equation tells us that $50x \equiv 150 \bmod 250$, i.e., that x is 3 mod 5. Hence x must be either 3 or 8 mod 10; from (a), we get that it's 8 mod 10.

The actual value of the discrete log, which is 248 by the way, could now be found by doing two more computations mod 5.

4. As in the previous problem, let $p = 251$ and let $g = 6 \bmod p$.

a. What are the quantities $\log_g(2) + \log_g(3)$ and $\log_g(2) + 3\log_g(5)$?

The first quantity is $\log_6(6)$, which is 1! The second quantity is $\log_g(250) = \log_g(p-1)$; this is $(p-1)/2 = 125$ because $g^{(p-1)/2} = -1$ whenever g is a generator (or, more generally, whenever g is replaced by a non-square).

As you can see, we're trying to do a baby version of index calculus in this problem: we want to get three equations for the three unknowns $\log(2)$, $\log(3)$ and $\log(5)$. In part (a), we get two equations without breaking a sweat, and now the aim is to get a third equation. You can imagine that the data in part (b) would come after some calculation....

b. Given the values $g^5 = 246$ and $g^{10} = 25 \bmod p$, and using the result of (**a**), find the logarithms $\log_g(2)$, $\log_g(3)$ and $\log_g(5)$.

The second value gives $2\log_g(5) = 10$, so $\log_g(5)$ is either 5 or $5 + (p-1)/2 = 130$. The first value shows you that $\log_g(246) = 5$, so that $\log_g(5)$ is *not* 5. Hence $\log_g(5) = 130$. Thus $\log_g(2) = 125 - 390 = 235$ and $\log_g(3) = 1 - 235 = 16$. (The logs are calculated mod $p - 1$.)

5. a. Find an expression for the probability P that 100 random integers between 1 and 5,000 are all different.

The number P is the product $\prod_{i=0}^{99}(1 - i/5000)$. This is a birthday paradox product analogous to the product in the displayed formulas at the top of page 228 of the textbook. According to sage, we have $P \approx 0.369$.

b. For all real numbers x, one has $1 - x \leq e^{-x}$. Exploiting this fact, establish an upper bound of the form e^{-r} for the probability P.

This would be e^{-r}, where $r = \sum_{i=0}^{99} i/5000 = (99 \cdot 100)/10000 = 99/100$. We have $e^{-r} \approx 0.3716$.

c. Is the upper bound in (**b**) adequate to decide whether or not P is less than $1/2$? (It might be helpful to remember that $\log 2$ is approximately 0.693.)

We have $e^{-r} < 1/2$ if and only if $r > \log 2$. This statement is true because $0.99 > 0.694$. The bound is adequate.

Note: the page http://amca01.wordpress.com/2010/04/02/playing-with-the-playfair-cipher/ presents an example where sage is used in cryptography.