Math 116

First Midterm Examination

February 18, 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.

Problem	Your score	Possible points
1		7 points
2		6 points
3		7 points
4		5 points
5		5 points
Total:		30 points

1. a. Find the greatest common divisor of 255 and 297. Write this gcd as an integral linear combination $t \cdot 255 + u \cdot 297$.

The gcd is $3 = 7 \cdot 255 - 6 \cdot 297$.

b. For which pairs of integers (a, b) is it possible to find an integer x such that

$$x \equiv \begin{cases} a & \bmod 255, \\ b & \bmod 297? \end{cases}$$

For example, can we find an x when $a = 4$, $b = 11$?

If x satisfies the two congruences, then 3 divides $x - a$ and also $x - b$, since 3 divides both 255 and 297. Hence 3 divides $a - b$, which means that we have $a \equiv b \bmod 3$. In particular, there can be no x when $a = 4$ and $b = 11$.

Conversely, suppose that $a \equiv b \bmod 3$. Then we can find an x that satisfies the two congruences, namely $x = a + (7 \cdot 255)\dfrac{b-a}{3}$. To see that this works, we can note that x is visibly of the form $a +$ a multiple of 255, so that x is $a \bmod 255$. Further, $7 \cdot 255 \equiv 3 \bmod 297$. Hence mod 297 we clearly have $x \equiv a + (b - a) = b$.

2. Let p be the prime number 103; note that $p - 1$ factors as $2 \cdot 3 \cdot 17$. What numbers occur as orders of elements of the group $\mathbf{F}_p^*$? How many elements of $\mathbf{F}_p^*$ are there of each order?

The possible orders are the positive divisors of $p - 1$, namely: 1, 2, 3, 17, $2 \cdot 3$, $2 \cdot 17$, $3 \cdot 17$ and $p - 1$. For each divisor d of $p - 1$, the number of elements of order d is $\varphi(d)$, where φ is the Euler phi function. These φ-values are respectively 1, 1, 2, 16, 2, 16, 32 and 32. The sum of these eight numbers is $102 = p - 1$, as we'd expect. (Each element has exactly one order!)

3. a. Find a square root of 19 mod 103. (No need to simplify your answer.)

Since $p = 103$ is 3 mod 4, a square root is $19^{(p+1)/4} = 19^{26}$. I am told that the value of this expression is 15 mod p. This makes sense because $15^2 = 225$ is $19 + 206 = 19 + 2 \cdot 103$.

b. How many elements of $(\mathbf{Z}/255\mathbf{Z})^*$ have square equal to 1? List three of these elements.

We saw above that 255 is divisible by 3, and it's clearly divisible by 5. It's $3 \cdot 5 \cdot 17$. Because 255 is the product of three distinct odd primes, there are $2^3 = 8$ square roots of 1 mod 255. Of course, 1 and -1 are square roots of 1 mod 255. To get a third square root of 1, we need to exhibit an "exotic" square root of 1. One way to do this is to look for a number that's 1 mod $5 \cdot 17 = 85$ and -1 mod 3. We don't have to look very far: 86 does the trick. You can check that $86^2 - 1$ is divisible by 255; it's $255 \cdot 29$, in fact.

4. Suppose that someone furnishes you with a table of the values of 5^{2^i} mod 144169 for $i = 0, \ldots, 10$. How would you compute 5^{821} mod 144169 in terms of those values? (Write an explicit formula.) If you write 821 as a sum of powers of 2, then 5^{821} gets written as a product of terms of the form 5^{2^i}. (Thinking in this way leads you to the "fast-powering algorithm.") The binary expansion of 821 is 1100110101, which means that $821 = 512 + 256 + 32 + 16 + 4 + 1 \ldots$

5. Bob and Alice agree to communicate with each other using a Diffie–Hellman key exchange. They select the prime number $p = 1237$ and the generator $g = 2$. Bob chooses his secret integer b and receives from Alice the value A.

a. What number should Bob send to Alice? (Write a formula — don't try to compute an explicit value.)

Bob sends Alice the value $B = 2^b$.

b. What computation does Bob perform to obtain the secret value that he and Alice will share?

He computes $A^b = 2^{ab}$, where a is Alice's secret value. Alice obtains the same number by computing B^a. Too bad for Eve.