Math 116

PROFESSOR KENNETH A. RIBET

Final Examination

May 19, 2009

8 AM–11 AM, 3 Evans 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 all questions, even computational ones, *show your work* and explain in complete sentences what you are doing. Think of this exam paper as your representative.

Problem	Your score	Possible points
1		6 points
2		8 points
3		8 points
4		7 points
5		4 points
6		9 points
7		8 points
Total:		50 points

1. Use the congruence $294^2 \equiv 10^2 \bmod 1349$ to find a non-trivial factorization of 1349.

You have to compute the gcd of 304 *or* 284 *with* 1349*. This is annoying, perhaps, but how bad can it be:*

$$1349 = 4 \cdot 304 + 133, \quad 304 = 2 \cdot 133 + 38, \quad 133 = 3 \cdot 38 + 19, \ldots.$$

The gcd is 19*, and* $1349 = 19 \cdot 71$.

2. a. Find numbers a and b so that

$$(-1,0) + (0,-1) + (a,b) = O$$

on the elliptic curve $y^2 + y = x^3 - x$ over the field of rational numbers.

The main point is that three distinct points on an elliptic curve sum to O (the point at infinity) if and only if they are collinear. If you ask that a and b satisfy $a + b = -1$ as well as $b^2 + b = a^3 - a$, you quickly get a cubic equation for a. The cubic has 3 as the sum of its roots, and two roots are already known, namely -1 and 0. Hence the remaining root is $a = 2$. This gives $b = -3$.

b. How many points does the elliptic curve $y^2 + y = x^3 - x$ have over the field with 2 elements? over the field with 3 elements?

Just count the possibilities for x and y, remembering to add in the point at infinity at the end. There are 5 point mod 2 and 7 points mod 3.

3. a. If an elliptic curve has 9 points over the field with 7 elements, how many points does it have over the field with 49 elements?

We did problems like this in class, and the answer here seems to be 63. Method: As in the book, write $9 = 1 + p - t = 8 - t$ and learn from this equation that $t = -1$. If α and β are the roots of $x^2 - tx + p$ (i.e., $x^2 + x + 7$), the number of points of the curve over $\mathbf{F}_7$ is $(1 - \alpha)(1 - \beta)$, and the number of points of the curve over $\mathbf{F}_{49}$ is $(1 - \alpha^2)(1 - \beta^2) = [(1 - \alpha)(1 - \beta)][(1 + \alpha)(1 + \beta)]$. The first factor is the 9 that we started with. The second factor is $1 + p + t = 8 + (-1) = 7$. Thus the product is $9 \cdot 7 = 63$.

b. On the elliptic curve $y^2+y = x^3-x$ over the field with 67 elements, the points $Q = (44, 33)$ and $R = (14, 33)$ have order 2. Determine the Weil pairing $e_2(Q, R)$.

Sorry for this annoying question. The values of the Weil pairing e_2 are 2nd roots of unity; they're either 1 or -1. If P_1 and P_2 are of order 2, $e_2(P_1, P_2) = 1$ if and only if P_2 is a multiple of P_1. But P_1 has only one non-zero multiple, namely itself. Hence in fact $e_2(P_1, P_2) = -1$ if P_1 and P_2 are distinct points of order 2. That's the case here, so the answer is -1.

4. Compute:

a. The probability of getting at least 4 heads when a fair coin is tossed 10 times.

The number of possible outcomes of this experiment is $2^{10} = 1024$. The number of ways of getting 0 heads is 1. (You have to go tail, tail,. . . .) The number of ways of getting one head is 10; for two heads the number is $(10 \cdot 9)/2 = 45$. For three, it's $(10 \cdot 9 \cdot 8)/6 = 120$. So my answer is the fraction whose numberator is $1024 - 166 = 858$ and whose denominator is 1024, or $143/17$ if you prefer. If you leave things in terms of binomial coefficients, that's probably OK, though I hope that you write the answer either as a single number or as an expression that can be computed by a sixth grader.

b. The number of integer triples (a, b, c) with $|a| \leq 5$, $|b| \leq 6$, $|c| \leq 7$.

I took this problem from a final exam at another university. The answer is the number of possible as times the number of possible bs times the number of possible cs. These numbers are 11, 13 and 15, so the answer is $11 \cdot 13 \cdot 15 = 2145$. (You don't have to compute 2145.)

5. Suppose that we wish to find t so that $2^t \equiv 72 \bmod 101$. If Pollard's ρ method yields the congruence $2^{10} \equiv 72^{10} \bmod 101$, what information can we obtain about the exponent t?

We have been provided with the congruence $2^{10} \equiv 2^{10t} \bmod 101$; note that 101 is a prime. We can infer that $10 \equiv 10t \bmod r$, where r is the order of 2 in $(\mathbf{Z}/101\mathbf{Z})^*$. Thus r is a divisor of 100, and we might as well go with the worst-case scenario, namely that $r = 100$. (If you understand from the context that 2 is a generator mod 101, you'll be on safe grounds, since there seems to be an understanding that t exists and that there's nothing special about 72. You can check, if you want that r is indeed 100. To see that $r = 100$, you need to know that 2 isn't a square mod 101, which follows from quadratic reciprocity, and also that 2 isn't a fifth power mod 101. To check this latter fact, you need to know that $2^{20} \not\equiv 1 \bmod 101$, and *you can probably see this with a non-horrible calculation. For the record, $2^{20} \equiv 95$ mod 101.) The congruence $10 \equiv 10t$ mod 100 is equivalent to $t \equiv 1$ mod 10; this is the intended answer. From the point of view of the DLOG problem, checking the values $t = 1, 11, 21, \ldots$ is much better than checking $t = 1, 2, \ldots$. The actual value of t is 41.*

6. Suppose that p is a prime $\equiv 5 \bmod 8$ and that a is a square mod p.

a. Show that either $a^{(p-1)/4} \equiv 1 \bmod p$ or $a^{(p-1)/4} \equiv -1 \bmod p$.

If $a = b^2$, say, then the square of $a^{(p-1)/4}$ is b^{p-1}, which is 1 mod p by Fermat's little theorem. On the other hand, if you have a number whose square is 1 (mod p), then the number can only be ± 1.

b. If $a^{(p-1)/4} \equiv 1 \bmod p$, show that $a^{(p+3)/8}$ is a square root of a mod p.

Squaring $a^{(p+3)/8}$ gives $a^{(p+3)/4} = a^{(p-1)/4} \cdot a^{4/4}$. The first term of the product is 1 by assumption; the second term is a.

c. If $a^{(p-1)/4} \equiv -1 \bmod p$, show that $2a \cdot (4a)^{(p-5)/8}$ is a square root of a mod p.

Square the purported square root, and you get a power of 2 times a power of a. The power of 2 is $2^2 \cdot 2^{(p-5)/2} = 2^{(p-1)/2} = -1$ because of quadratic reciprocity (and the assumption $p \equiv 5$ mod 8). The power of a is $a^2 \cdot a^{(p-5)/4} = a \cdot a^{(p-1)/4} = -a$, since we are assuming that $a^{(p-1)/4} = -1$ in the world of numbers mod p. The problem works out because $(-1)(-a) = a$.

7. While studying Math 116 together in 1015 Evans, Alice and Bob work out some examples using an RSA modulus n that they found in a textbook. Because they have become comfortable with n, Alice and Bob retire to their dorm rooms and publish public RSA keys that each use the modulus n as part of their the public key. Assume that they choose different public encryption keys e_A and e_B; in fact, suppose that $\gcd(e_A, e_B) = 1$.

Imagine now that Nancy sends the same secret message to Alice and to Bob by using RSA encryption and the two public keys. Suppose also that Eve anticipates that Nancy will be sending the same plaintext to Bob and Alice and that Eve intercepts the two different encryptions of the common plaintext message. Show that Eve can recover the plaintext by multiplying together suitable powers of the two intercepted ciphertexts. [Hint: write 1 as a sum of a multiple of e_A and a multiple of e_B.]

Follow the hint and write $1 = re_A + se_B$. Nancy sends, and Eve receives, m^{e_A} and m^{e_B} (mod n), where m is Nancy's plaintext. Eve computes (mod n):

$$(m^{e_A})^r (m^{e_B})^r = m^{re_A + se_B} = m^1 = m$$

and thus recovers the plaintext. In crypto jargon, there has been a "failure of protocol." Alice and Bob messed up.