Math 116

PROFESSOR KENNETH A. RIBET

Final Examination

May 13, 2010

8 AM–11 AM, 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		9 points
2		8 points
3		5 points
4		4 points
5		8 points
6		8 points
7		8 points
Total:		50 points

1. Bob publishes as his private key the RSA modulus $n = 4087 = 61 \cdot 67$ and the exponent $e = 17$. Bob's friend Alice wishes to send him a non-zero integer m mod n in a secure manner.

a. Alice checks that the $\gcd(m, n)$ is 1. Had this gcd been > 1, what urgent unencrypted message would Alice have sent to Bob?

YOU IDIOT: YOUR RSA MODULUS IS NOT SECURE. CHANGE IT IMMEDIATELY!!

b. What arithmetic operation does Alice perform to produce the encrypted message c that she will send to Bob?

She computes $c = m^e$.

c. Bob recovers m by raising c to a certain power. What power?

The inverse of e mod $(61 - 1)(67 - 1) = 3960$. This inverse is calculated by the Euclidean algorithm and turns out to be 233: $3960 = 17 \cdot 232 + 16 = 17 \cdot 233 - 1$ and thus $17 \cdot 233 = 1 + 3960$.

2. a. In the following transcript, what output does `sage` produce when `(a^2 + 2*a + 2)^2` is input?

```
sage: 1+1 #the input occurs on the lines beginning "sage:"
2
sage: K.<a> = GF(27); K
Finite Field in a of size 3^3
sage: a.minimal_polynomial()
x^3 + 2*x + 1
sage: (a^2 + 2*a + 2)^2
```

We have $a^3 + 2a + 1 = 0$, i.e., $a^3 = a - 1$. Then

$(a^2 + 2a + 2)^2 = a^4 + 4a^3 + 8a^2 + 8a + 4 = a^4 + a^3 - a^2 - a + 1 = (a^2 - a) + (a - 1) - a^2 - a + 1 = -a = 2a.$

b. The session continues as follows:

```
sage: EllipticCurve('11a').change_ring(GF(3)).order()
5
sage: EllipticCurve('11a').change_ring(K).order()
```

What number does `sage` output in response to the second command?

In other words, if an elliptic curve has 5 points over the field with 3 elements, how many points does it have over the field with 27 elements? The same type of problem was on the exam last year. As explained in the textbook, one writes $\#E(\mathbf{F}_p) = (1 - \alpha)(1 - \beta)$, where $\alpha\beta = p$ and $\alpha + \beta = 1 + p - \#E(\mathbf{F}_p)$; here $p = 3$ and E is the curve in question. Hence $\alpha + \beta = 4 - 5 = -1$. We are looking for $\#E(\mathbf{F}_{p^3})$, which is then $(1-\alpha^3)(1-\beta^3) = 1+p^3-(\alpha^3+\beta^3) = 28-(\alpha^3+\beta^3)$. Now $-1 = (-1)^3 = (\alpha+\beta)^3 = \alpha^3+\beta^3+3\alpha\beta(\alpha+\beta) = \alpha^3 + \beta^3 - 9$, so that $\alpha^3 + \beta^3 = 8$. Hence the answer is $28 - 8 = 20$.

3. We continue some calculations begun in problem 4 of the second midterm:

```
sage: p=251; R=Integers(p); g = R(6); h= R(242)
sage: log(R(2),g); log(R(3),g); log(R(5),g)  # cf. solutions to MT2
235
16
130
sage: for i in range(15):  # 15 is around the square root of p
...       print(i, h*g^(-i))
(0, 242)
(1, 124)
(2, 188)
(3, 115)
(4, 61)
(5, 52)
(6, 176)
(7, 113)
(8, 228)
(9, 38)
(10, 90)
(11, 15)
(12, 128)
(13, 105)
(14, 143)
```

Find the discrete logarithm $\log_g(h)$.

We notice, for example, that $hg^{-11} = 15 = 3 \cdot 5$, so that $\log h - 11 = \log 3 + \log 5 = 16 + 130$. Hence $\log h = 11 + 16 + 130 = 157$.

4. Find the greatest common divisor $\gcd(2^{i!} - 1, 47 \cdot 73)$ for the four values $i = 5$, 10, 15 and 25. (It may be helpful to know that $5^8 - 2 = 73 \cdot 5351$.)

Let n be the order of 2 mod 47 and let m be the order of 2 mod 73. The gcd is 1 if $i!$ is divisible by neither n nor m and $47 \cdot 73$ is $i!$ is divisible by both of these numbers. If $i!$ is divisible only by n, then the gcd will be 47 and similarly for divisibility by m. So we know the answer as soon as we figure out n and m.

Since $46 - 1 = 2 \cdot 23$, the only possibilities for n a priori are 1, 2, 23 and 46. Clearly, 4 isn't congruent to 1 mod 47, so the order must be 23 or 46. If it's 23, then 2 is a square mod 47, but we know by quadratic reciprocity (since $47 \equiv 5$ mod 8) that 2 is a non-square mod 47. Hence the order really is 46. As will presumably become apparent, it doesn't really matter whether the order is 23 or 46 since $i!$ is divisible by 23 if and only if it's divisible by 46.

To find m looks like more trouble, since 72 has lots of factors! However, the "helpful to know" congruence $5^8 \equiv 2$ mod 73 shows that 2 is already an eighth power mod 73. Hence the order of 2 mod 73 divides 9: it must be 1, 3 or 9. Since 2^3 clearly isn't congruent to 1 mod 73, the order is 9. In sum: $m = 9$.

Now $i!$ is divisible by 9 if and only if $i \geq 6$. Also, $i!$ is divisible by 23 if and only if $i \geq 23$. Thus the four gcd's are respectively: 1, 73, 73, $47 \cdot 73$.

5. a. Compute the sum of the two points $(-1, 0)$ and $(1, 2)$ on the elliptic curve $y^2 = x^3 + x + 2$ over the field of rational numbers.

This is basically a repeat of a problem from last year's exam that we discussed in class 9 days ago. The line through the two points is easily found to have equation $y = x + 1$. To see where the line meets the elliptic curve, you have to solve $(x+1)^2 = x^3 + x + 2$. Collect all the terms to one side, and you get $x^3 - x^2 + \cdots = 0$. Hence the sum of the roots is 1 (the negative of the coefficient of x^2). Since -1 and 1 are already roots, the third root is 1, so the third point of intersection is $(1, 2)$. To get the sum on the elliptic curve, change the sign of the y-coordinate; we get $(1, -2)$.

b. On the elliptic curve $y^2 + y = x^3 - x^2$ over $\mathbf{Q}$, the point $P = (0, 0)$ has order 5; its non-zero multiples are $2P = (1, -1)$, $3P = (1, 0)$ and $4P = (0, -1)$. What is the value of the Weil pairing $e_5(P, 2P)$?

Well, $e_5(P, 2P) = e_5(P, P)^2$ by the linearity of the Weil pairing, but the number $e_5(P, P)$ is 1 because the Weil pairing is alternating. Hence the value is 1. By the way, to see a nice photo of a point of order 5 on an elliptic curve, check out http://math.stanford.edu/seminars/Serre_poster.pdf. The first of three talks will be given tomorrow (down at the Farm).

6. Assume that $p > 2$ is a prime number and that a is a non-zero square mod p.

a. Show that there are exactly two square roots of a mod p, each one the negative of the other.

If a is a square, it's b^2 for some b. A square root of a is a number s such that $s^2 = a = b^2$. The equation $s^2 = b^2$ among numbers mod p may be rewritten $(s - b)(s + b) = 0$. It certainly holds if $s = \pm b$. Conversely, because $\mathbf{Z}/p\mathbf{Z}$ is a field, if it holds then one of the two factors must be 0; we must have $s = \pm b$. Thus the square roots of a are the numbers $+b$, $-b$. They are distinct because of $b = -b$ we have $2b = 0$ and thus $b = 0$ because p is odd. And, of course, once b is 0 then a is 0 as well, but we have insisted that a be non-zero when we began.

b. If $p \equiv 3$ mod 4, explain why $a^{(p+1)/4}$ is a square root of a mod p.

Square the number to get $a^{(p+1)/2} = a^{(p-1)/2} \cdot a$. Because a is a square, the first factor is 1 by Fermat's Little Theorem.

c. Suppose now that $p \equiv 5 \bmod 8$. Show that $a^{(p-1)/4}$ is either $+1$ or -1. In the former case, show that $a^{(p+3)/8}$ is a square root of a mod p.

If you square $a^{(p-1)/4}$, you get $a^{(p-1)/2}$, which is 1 (as we just said). Hence $a^{(p-1)/4}$ must be a square root of 1, i.e., either $+1$ or -1. Assume that it's $+1$ and square $a^{(p+3)/8}$. The result is $a^{(p+3)/4} = a \cdot a^{(p-1)/4} = a$.

d. In the latter case, show that $2a \cdot (4a)^{(p-5)/8}$ is a square root of a mod p.

If you square the number, you get $4a^2 \cdot 4^{(p-5)/4} \cdot a^{(p-5)/4} = 2^{(p-1)/2} \cdot a \cdot a^{(p-1)/4} = -2^{(p-1)/2}a$. However, $2^{(p-1)/2} = -1$ by quadratic reciprocity, so the product simplifies to a. If you have studied the Tonelli–Shanks algorithm, you know that you start the algorithm by finding a non-square mod p. In general, you pick a random number mod p, check to see whether it's a non-square and then move on to another random number if it's in fact a square. In this situation, 2 is a non-square, so we don't have to make random picks, and the equation $p - 1 = 4 \cdot (p-1)/4$ expresses $p - 1$ as the product of a power of 2 and an odd number.

7. Roughly 0.8 percent of all 175-bit positive integers are prime. Imagine a test for primality that returns "prime" for 7 percent of composite numbers and 90 percent of prime numbers; it returns "composite" otherwise. (Thus the test issues false positives and false negatives.) If a 175-bit positive integer is declared to be prime by this test, what is the probability that the integer is indeed a prime number?

[This problem is a paraphrase of a question about medical testing that was discussed in an April 15 New York Times blog post "Chances Are" by the Cornell mathematician Steven Strogatz. The blog explains that most doctors got the question wrong; one doctor became "visibly nervous" when seeing it. You can do better—Go Bears!]

Our probability space Ω is the set of 175-bit positive integers with the uniform distribution. Let's consider the following two events: T is the set of integers in Ω that the test says are prime; A is the set of integers in Ω that are actually prime. Let C (for "composite" or "complement") be the complement of A in Ω. Our aim is to calculate the conditional probability $\text{Prob}(A|T) = \dfrac{\text{Prob}(A \cap T)}{\text{Prob}(T)}$.

We have

$$\text{Prob}(T \cap A) = \text{Prob}(T|A)\,\text{Prob}(A),$$

where both factors are known to us. Similarly,

$$\text{Prob}(T \cap C) = \text{Prob}(T|C)\,\text{Prob}(C),$$

and again both factors in the product are given to us in the problem. Also,

$$\text{Prob}(T) = \text{Prob}(T \cap A) + \text{Prob}(T \cap C)$$

because T is the disjoint union of the two subsets in question. Hence we know both the numerator and denominator of the fraction $\text{Prob}(T \cap A) = \text{Prob}(T|A)\,\text{Prob}(A)$ and can thus get the answer by subsituting in numbers.

If I'm not mistaken, $\text{Prob}(T \cap A) = 0.9 \cdot 0.008$ and $\text{Prob}(T \cap C) = 0.07 \cdot 0.992$, so that

$$\text{Prob}(T) = 0.9 \cdot 0.008 + 0.07 \cdot 0.992 = 0.07664.$$

Thus our answer is $(0.9 \cdot 0.008)/0.07664 \approx 0.0939$, which is a little over 9.3 percent. Of course, you don't have to simplify your answer, so writing the probability as a fraction involving a product and a sum of products is fine.