Math 116

PROFESSOR KENNETH A. RIBET

Final Examination

May 9, 2012

11:30 AM–2:30 PM, 9 Evans Hall

Please put away all books, calculators, cell phones and other devices. You may consult a single two-sided sheet of notes. Please write carefully and clearly in *complete sentences.* Take pain to explain what you are doing since your exam book is your only representative when your work is being graded.

Please hand in this page with your exam book. The questions along with skeletal solutions will be available on the course web page.

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

1. On the elliptic curve $y^2 + y = x^3 + 100x^2 + 91x + 81$ over the field $\mathbf{F}_{101}$, the points $P = (16, 60)$ and $Q = (43, 75)$ each have order 5. According to `sage`, the value of the Weil pairing $e_5(P, Q)$ is 87. Compute $e_5(P + 2Q, P + 4Q)$.

If $z = e_5(P, Q)$, then $e_5(P + 2Q, P + 4Q) = z^{1\cdot 4-1\cdot 2} = z^2$ because e_5 is an alternating (bilinear) function on $E[5]$ (Theorem!5.38). Hence the correct answer is 87^2 mod 101. This is a perfectly fine answer, but I imagine that many students will try to compute this square mod 101. Because $87 \equiv -14$, $87^2 \equiv 4 \cdot 49 = 2 \cdot 98 \equiv -6 \equiv 95$.

2. Bob sends Alice a binary string that includes 85% 0's and 15% 1's. Random transmission errors alter 20% of the bits. Alice receives '1' as the 116th bit. What is the probability that the 116th bit was in fact sent as a '1'?

Let "Pr" stand for "probability." Let E be the event that a 1 was sent and E' (the complement of E) be the event that a 0 was sent. Let F be the event that a 1 was received. We seek to compute

$$\Pr(E|F) = \frac{\Pr(E \cap F)}{\Pr(F)}$$

and note that the denominator $\Pr(F)$ is the sum $\Pr(F \cap E) + \Pr(F \cap E')$.

We have $\Pr(F \cap E) = \Pr(F|E)\Pr(E) = 0.8 \cdot 0.15$ and $\Pr(F \cap E') = \Pr(F|E')\Pr(E') = 0.2 \cdot 0.85$. Thus $\Pr(E|F) = \dfrac{0.8 \cdot 0.15}{0.8 \cdot 0.15 + 0.2 \cdot 0.85} = \dfrac{12}{29}$. The decimal value of this fraction is approximately 0.414.

3. Let E be the elliptic curve $y^2 = x^3 - x$ over the field with 7 elements. Find the orders of the two groups $E(\mathbf{F}_7)$ and $E(\mathbf{F}_{7^2})$.

The curve has $7 + 1 = 8$ points over $E(\mathbf{F}_7)$, as you can see by counting: For $x = 0, 1, -1$, there is one point, corresponding to $y = 0$. There are four remaining values of x; two are such that $x^3 - x$ is a non-zero square, and thus yield two points on the curve, and two are such that $x^3 - x$ is a non-square and thus yield no points on the curve. This gives 7 points, but there is also O. Using Theorem 5.29, which I hope you all read the night before the exam after receiving my email message, one sees that there are 64 points on the curve over $E(\mathbf{F}_{7^2})$.

4. Let p and q be the prime numbers 2003 and 4001, and let $N = pq$. If (x_i) is the sequence mod p defined by $x_0 = 1$ and $x_{i+1} = x_i^2 + 1$ ($i \geq 0$), the first collision in the sequence occurs for the indices 39 and 54. (We have $x_{39} = x_{54} = 424$.) If (y_i) is the sequence analogous to (x_i) with p replaced by q, the first collision occurs for the indices 37 and 52; we have $y_{37} = y_{52} = 3699$. Let (z_i) be the sequence analogous to (x_i) and (y_i) in which we work mod N (rather than mod p or mod q).

View the z_i as positive integers between 0 and $N - 1$. Describe the sequence

$$\gcd(N, z_i - z_{2i}), \quad i = 0, 1, \ldots.$$

The z-sequence becomes the x-sequence mod p and the y-sequence mod q. Mod p, we have $x_i = x_j$ for $i \leq j$ if and only if $j \equiv i \bmod 15$ and $i \geq 39$. Hence $x_i = x_{2i}$ if and only if i is divisible by 15 and at least 45 (or equal to 0). A completely analogous statement can be made for the y-sequence because $52 - 37 = 15$. Thus the gcd in the problem is N for i divisible by 15 and $i \geq 45$. It's N also when $i = 0$. Otherwise it's 1. The point of this problem is that the Pollard ρ method does not factor N if we use the simple $x^2 + 1$ recursion in the problem. Of course, we could try with another function, for instance $x^2 + 2$.

```
print N
x=Mod(1,N)
y=Mod(1,N)
for i in range(1,100):
    x=x^2+1
    y = (y^2+1)^2+1
    print i, gcd(N,ZZ(x-y))
```

5. Suppose that p is the prime number 107 and that g is the primitive root 2 mod p. Using the congruences

$$2^{34} \equiv 9 \pmod{p}, \qquad 2^{11} \equiv 15 \pmod{p},$$

find the discrete logarithms $\log_g 3$ and $\log_g 5$.

Say $2^x = 3$ in $\mathbf{F}_p$. Then $2^{2x} = 9 = 2^{34}$, giving $2x \equiv 34$ mod 106. Hence $x \equiv 17$ mod 53, so that $x = 17$ or $x = 70$. (Note that x is a number mod $106 = p - 1$.) If $3 = 2^{17}$, then 3 is a non-square mod p, while if $3 = 2^{70}$ then 3 is a square mod p. In fact, quadratic reciprocity shows that 3 is indeed a square mod 107, so that $\log_g 3 = 70$.

```
sage: g=Mod(2,107)
sage: three=Mod(3,107)
sage: log(three,g)
70
```

We then find that $\log_g 5 = 47$.

6. Explain why elliptic curve discrete log problems are considered more secure than multiplicative discrete log problems of the same bit size.

You'll get most or all of the points if you write something about index calculus. Answers will be judged on their brevity, use of complete sentences with good grandma and other criteria of high school English courses.

7. Consider the following `sage` transcript:

```
sage: p=127
sage: g=Mod(46,p)
sage: h=Mod(43,p)
sage: n = floor(sqrt(p-1))+ 1 # useful for baby-step... algorithm
sage: p-1 == g.multiplicative_order()
True
sage: v=[(g^i,i, ’baby’) for i in range(n)]
sage: v[:4] # print out the beginning of this list
[(1, 0, ’baby’), (46, 1, ’baby’), (84, 2, ’baby’), (54, 3, ’baby’)]
sage: w = [(h*g^(-n*j),j,’giant’) for j in range(12)]
sage: w[:3] # a small bit of w
[(43, 0, ’giant’), (83, 1, ’giant’), (110, 2, ’giant’)]
sage: z=v+w # concatenates the two lists
```

```
sage: z.sort() # sorts the result
sage: z[14:18] #prints some of the sorted concatenation
[(90, 6, 'giant'), (91, 5, 'baby'), (91, 5, 'giant'), (93, 11, 'giant')]
```

Find the log of h with respect to g.

The answer, according to a sage calculation that I just ran, is 65. I hope that you all get this answer from the data provided: We know that $g^5 = 95 = hg^{-5n}$, so that $h = g^{5n+5}$. Clearly, $n = 12$, so we do get 65. Phew!

8. Let p be an odd prime number. Suppose that a and n are numbers mod p for which $a^2 - n$ is not a square mod p. Let $\mathbf{F} = \mathbf{F}_{p^2}$ be the field obtained by adjoining the square roots of $a^2 - n$ to $\mathbf{F}_p$ and let s be a square root of $a^2 - n$ in $\mathbf{F}$. Show that $(a + s)^{(p+1)/2}$ is a square root of n in F. If n is a square mod p, prove that $(a + s)^{(p+1)/2}$ lies in $\mathbf{F}_p$.

This problem was based on the lecture of February 28, 2012. We are looking at Cipolla's algorithm `http://en.wikipedia.org/wiki/Cipolla's_algorithm`. To show that $(a+s)^{(p+1)/2}$ is a square root of n in F, we square $(a + s)^{(p+1)/2}$, getting

$$(a + s)^{p+1} = (a + s)^p(a + s) = (a^p + s^p)(a + s)$$

because the pth power map is additive when $p = 0$. Now $a^p = a$ by Fermat's little theorem. Also,

$$s^p = s^{p-1}s = (s^2)^{(p-1)/2}s = (a^2 - n)^{(p-1)/2}s = -s.$$

In the last equality, we use that $t^{(p-1)/2} = -1$ if t is a non-square mod p. (I couldn't find an obvious reference for this fact in the book, but this fact was mentioned in class, as I verified right before the exam.) Hence

$$(a + s)^{p+1} = (a - s)(a + s) = a^2 - s^2 = a^2 - (a^2 - n) = n,$$

which gives the first assertion. For the second: Because n is a square mod p, it has two square roots in $\mathbf{F}_p$. It has at most two square roots in $\mathbf{F}_{p^2}$. Hence if we have a square root of n in $\mathbf{F}_{p^2}$ it actually has to be one of the two square roots of n in $\mathbf{F}_p$.