Math 116

PROFESSOR KENNETH A. RIBET

Last Midterm Examination

March 20, 2012

9:40AM–11:00 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 midterm questions (and answers, after a while) will be available on the course web page.

Your NAME: _____

Problem	Your score	Possible points
1		5 points
2		5 points
3		10 points
4		7 points
5		8 points
Total:		35 points

1. Using the Jacobi symbol, show that 7 is not a square mod 5893.

Because 5893 is 1 mod 4, quadratic reciprocity for the Jacobi symbol gives $\left(\frac{7}{5893}\right) = \left(\frac{5893}{7}\right) = \left(\frac{6}{7}\right) = -1$. Hence 7 is not a square mod 5893. Of course, we know that it's possible to have $\left(\frac{a}{N}\right) = +1$ in situations where a is not a square mod N. For example, 13 is not a square mod 5893, but we have nonetheless $\left(\frac{13}{5893}\right) = 1$.

2. Given the congruences $67^2 \equiv -144 \bmod 4633$ and $68^2 \equiv -9 \bmod 4633$, what gcd would you compute in an attempt to factor 4633?

We have $(67 \cdot 68)^2 \equiv (3 \cdot 12)^2 \bmod 4633$. The natural thing to do is to compute $\gcd(67 \cdot 68 \pm 36, 4633)$; computing one of the two is no better than computing both. I just did this: with the minus sign, the gcd is 113. With the plus sign, the gcd is 41. We have $4633 = 41 \cdot 113$.

3. Let $N \geq 2$ be an integer. Suppose that $N-1$ is divisible by a prime number $q > \sqrt{N} - 1$. Suppose further that there is an integer a for which $a^{N-1} \equiv 1 \bmod N$ and $\gcd(a^{(N-1)/q} - 1, N) = 1$. Prove that N is a prime number, writing a proof that follows this outline:

(1) Assume that N is not a prime. Then there is a prime $p \leq \sqrt{N}$ that divides N.
(2) We have $q > p - 1$, and therefore q and $p - 1$ are relatively prime.
(3) There exists an integer u such that $uq \equiv 1 \bmod p - 1$.
(4) We have $a^{(N-1)/q} \equiv a^{(N-1)u} \equiv 1 \bmod p$, which contradicts the assumption that $a^{(N-1)/q} - 1$ is relatively prime to N.

We seek to prove that N is prime. We suppose the contrary, so that N is product ef with $1 < e, f < N$. At least one of e, f is $\leq \sqrt{N}$. Taking a prime divisor of the relevant factor, we find that N is dividible by a prime number $p \leq \sqrt{N}$. Since $q > \sqrt{N} - 1$, we have $q > p - 1$. Because q is prime, the gcd of q and $p - 1$ is then 1. This means that q has an inverse mod $p - 1$. Let u be this inverse, considered as an integer between 1 and $p - 2$.

Note that a is not divisible by p because $a^{N-1} \equiv 1 \bmod N$ and N is a multiple of p. Therefore, $a^{p-1} \equiv 1 \bmod p$ by Fermat's Little Theorem. Accordingly, if i is an integer, the value of $a^i \bmod p$ depends only on the residue class of $i \bmod p-1$. We thus have $a^{(N-1)/q} \equiv a^{(N-1)u} \equiv 1 \bmod p$ because $(N-1)/q$ and $(N-1)u$ are congruent mod $p-1$ and because of the assumption $a^{N-1} \equiv 1 \bmod N$, which implies that a^{N-1} is 1 mod p. Thus $a^{(N-1)/q} - 1$ is divisible by p, which is a factor of N, so that $\gcd(a^{(N-1)/q} - 1, N) \neq 1$, in contradiction with one of the hypotheses.

4. Let E be the elliptic curve defined by the equation $y^2 = x^3 + 3x + 4$ over the field $\mathbf{F}_{59}$ and let P be the point $(0, 2)$ in $E(\mathbf{F}_{59})$. Verify that $2P = (19, 28)$. Given the additional information that $3P$ has order 9, find the order of the group $E(\mathbf{F}_{59})$.

To check that $2P = (19, 28)$, use the formulas of Theorem 5.6 (p. 285 of the textbook). Once you know that $3P$ has order 9, you can conclude that P has order 27. This implies that the order of $E(\mathbf{F}_{59})$ is a multiple of 27. On the other hand, by Hasse's theorem, it differs from Hence the order lies between 45 and 75. The only multiple of 27 in this range is 54, so there are exactly 54 $\mathbf{F}_{59}$-rational points on E.

5. If p and q are the prime numbers 189843751 and 569531279, then $p-1 = 2 \cdot 3^5 \cdot 5^8$, while $(q-1)/2$ is the prime number 284765639. Note that both p and q are congruent to 7 mod 8.

(1) Compute the order of 2 mod q.
(2) Show that 35! is a multiple of $p - 1$.
(3) Channelling Pollard's $p - 1$ method, prove that $\gcd(2^{35!} - 1, pq) = p$.
(4) A sage computation shows that $\gcd(2^{25!} - 1, pq) = p$. Using this fact, along with the congruence $p \equiv 7 \bmod 8$, show that the order of 2 mod p divides $3^5 \cdot 5^6$.

The order of 2 mod q is a divisor of $q - 1 = 2 \cdot 284765639$. This order is clearly not 1 or 2 because we don't have $4 \equiv 1 \bmod q$. Hence it's either $q - 1$ or 284765639. However, 2 is a square mod q because q is 7 mod 8. Hence the order of 2 actually divides 284765639 and must then be equal to 284765639.

For the second item, we have to show that 35! is divisible by 2,3^5 and 5^8 I'll leave the first two divisibilites to you. For the last, note that the product 35! includes 7 numbers divisible by 5 as well as the number 25, which contributes an additional factor of 5.

For the third item, we note that $2^{35!}$ is 1 mod p because of Fermat's Little Theorem and the divisibility we just proved. On the other hand, 35! is not divisible by the large prime number 284765639, which we have seen to be the order of 2 mod q. Hence $2^{35!}$ is *not* 1 mod q. Thus $2^{35!} - 1$ is divisible by p but not by q, which proves the required gcd statement.

For the final item, we learn from sage that the order of 2 mod p is a divisor of 25!. Because p (just like q) is 7 mod 8, this order divides $(p-1)/2 = 3^5 \cdot 5^8$. Hence it divides $\gcd(25!, 3^5 \cdot 5^8)$, which is easily seen to be $3^5 \cdot 5^6$. PS: Sage tells me that the order is in fact $3^5 \cdot 5^5$.