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.

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?

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 detailed 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.

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 $E(\mathbf{F}_{59})$.

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 $3^5 \cdot 5^6$.