Math 115 Professor K. A. Ribet
First Midterm Exam September 23, 1999

This is a closed-book exam: no notes, books or calculators are allowed. Explain your answers in complete English sentences. No credit will be given for a "correct answer" that is not explained fully.

**1** *(4 points). Find the remainder when* $2^{33}$ *is divided by 31.*

By Fermat's Little Theorem, $2^{31} \equiv 2 \bmod 31$. Thus $2^{33} \equiv 8 \bmod 31$.

**2** *(4 points). Use the identity* $27^2 - 8 \cdot 91 = 1$ *to find an integer* $x$ *such that* $27x = 14$ *mod 91.*

The identity shows that $27^2 \equiv 1 \bmod 91$. Hence $27^2 \cdot 14 \equiv 14 \bmod 91$. We can take $x$ to be $378 = 27 \cdot 14$ or any integer equivalent to $27 \cdot 14 \bmod 91$. In fact, you can check that 14 is the smallest positive integer that is congruent mod 91 to 378. This means that we have $27 \cdot 14 \equiv 14 \bmod 91$, so that $26 \cdot 14 \equiv 0 \bmod 91$. This may seem strange until one notes that $91 = 7 \times 13$. Hence $26 \times 14$ is indeed a multiple of 91.

**3** *(4 points). Find all prime numbers* $p$ *such that* $p^2 + 2$ *is prime.*

Maybe this is a silly question; I got it out of a book. If you try the first few primes, you see that $2^2 + 2 = 6$ isn't prime, that $3^2 + 2 = 11$ is prime, and that $5^2 + 2 = 27$ isn't prime. Trying a few more, you get the idea that $p^2 + 2$ is divisible by 3 for $p > 3$. This is clearly a true statement because any $p > 3$ is $\pm 1$ mod 3, so that its square is 1 mod 3. Thus $p^2 + 2$ is zero mod 3.

**4** *(5 points). Suppose that* $ax + by = 17$, *where* $a$, $b$, $x$ *and* $y$ *are integers. Show that the numbers* $\gcd(a, b)$ *and* $\gcd(x, y)$ *are divisors of 17. Decide which, if any, of the following four possibilities can occur:*

*(i)* $\gcd(a, b) = \gcd(x, y) = 1$;
*(ii)* $\gcd(a, b) = 17$ *and* $\gcd(x, y) = 1$;
*(iii)* $\gcd(a, b) = 1$ *and* $\gcd(x, y) = 17$;
*(iv)* $\gcd(a, b) = \gcd(x, y) = 17$.

If $d$ is a divisor of $a$ and $b$, then $d$ divides $ax$ and $by$, so it divides their sum, which is 17. Thus all divisors of $a$ and $b$ are divisors of 17; this applies, in particular to the gcd of $a$ and $b$. The gcd can only be 1 or 17, then. A similar statement applies to the pair $(x, y)$. Clearly, if 17 divides all of $a$, $b$, $x$, $y$, then $17^2$ divides $ax$ and $by$; this is impossible because $ax + by = 17$ is not divisible by $17^2$. Thus (iv) cannot occur. The other possibilities do, in fact, occur, however: If $x = y = 1$, $a = 16$ and $b = 1$, then we're in situation (i). If $x = y = 1$, $a = 17$ and $b = 0$, we're in situation (ii). Situation (iii) is the same as (ii) with the two pairs $(a, b)$ and $(x, y)$ reversed.

**5** *(6 points). Suppose that $n$ is composite: an integer greater than 1 that is not prime. Show that $(n-1)!$ and $n$ are not relatively prime. Prove that the congruence $(n-1)! \equiv -1 \bmod n$ is false.*

If $n$ is composite, it has a divisor $d$ that is bigger than 1 and less than $n$. The number $d$ is a factor of $(n-1)!$ because it's one of the numbers between 1 and $n-1$. Thus $n$ and $(n-1)!$ have a non-trivial common factor and therefore they are not relatively prime. The Wilson-type congruence is false because two numbers that are congruent mod $n$ must have the same gcd with $n$. The number $-1$ has gcd 1 with $n$, whereas $(n-1)!$ has a bigger gcd with $n$. The point of this problem is to show that there's a converse to Wilson's theorem; $n$ is therefore prime if and only if $(n-1)!$ is $-1$ mod $n$

**6** *(6 points). Prove that $-1$ is not a square modulo the prime $p$ if $p \equiv 3$ mod 4.*

This was covered in class and is explained in our textbook (p. 54).

**7** *(6 points). Show that $x^8 \equiv 1$ mod 20 if $x$ is an integer that is prime to 20. Find the integer $t$ such that $t^9 = 760231058654565217 \approx 7.60231 \times 10^{17}$.*

Well, I did promise to give you a problem like this! Euler's theorem states that $x^{\varphi(n)} \equiv 1 \bmod n$ for all $x$ prime to $n$. You can check quickly that $\varphi(20) = 8$: if you look at the numbers between 0 and 19 and take away those that are even or are divisible by 5, you have only eight of them that are left (namely: 1, 3, 7, 9, 11, 13, 17 and 19). Thus we do indeed have $x^8 \equiv 1$ mod 20 for $x$ prime to 20. Now if $t^9 = 760231058654565217$, then clearly $t$ must be odd and prime to 5. Thus $t^8 \equiv 1$ and $t^9 \equiv t$ mod 20. We visibly have $t^9 \equiv 17$ mod 20, so $t \equiv 17$ mod 20 as well. Next, note that $t$ is less than $100 = 10^2$, since $t^9 < 10^{18}$. Thus the only possible values of $t$ are 17, 37, 57, 77, and 97. In fact, $t = 97$. To see this, we can note that $80^9 \approx 1.34218 \times 10^{17}$ is a lot smaller than $t^9$; for this, you have to think about $8^9$, which is $1024 \times 1024 \times 128$. Alternatively, you can rule out 77 by noting that $t^9$ is not divisible by 11 (alternate sum of digits rule) and rule out 57 by noting that $t^9$ is not divisible by 3 (sum of digits rule). Once you do this, you can rule out 17 and 37 by checking that $40^9$ is a lot less than $10^{17}$.