Math 261 — Fall 2001–2002
Solutions to Midterm Quiz

1. Find the prime factorizations of 8536 and 7007, and use these to calculate $\varphi(7007)$ and the GCD $(8536, 7007)$.

Answer. $8536 = 2^3 \cdot 11 \cdot 97$, where 97 is prime since it is not divisible by any prime less than $\sqrt{97} \approx 10$. Also $7007 = 7^2 \cdot 11 \cdot 13$. We use this to conclude that $\varphi(7007) = (7^2 - 7)(11-1)(13-1) = 5040$, and that $(8536, 7007) = 11$.

2. Calculate $\left(\frac{3}{11}\right)$ in two ways, first by Euler's criterion, and second by Gauss' Lemma (not by quadratic reciprocity).

Answer. Note that $(11-1)/2 = 5$. Then Euler's criterion gives $\left(\frac{3}{11}\right) \equiv 3^5 \equiv 243 \equiv +1 \pmod{11}$. For Gauss' Lemma, we look at $3 \cdot 1 \equiv 3$, $3 \cdot 2 \equiv -5$, $3 \cdot 3 \equiv -2$, $3 \cdot 4 \equiv 1$, and $3 \cdot 5 \equiv 4 \pmod{11}$. Here we reduce to a residue mod 11 that is between ± 5. There are two minus signs (-5 and -2), so the quadratic residue is $(-1)^2 = +1$.

3. Find one solution to the equation $x^2 \equiv 5 \pmod{11^2}$. (You do not need to find the most general solution.)

Answer. If $x^2 \equiv 5 \pmod{11^2}$, then certainly $x^2 \equiv 5 \pmod{11}$. So we can start with $x_0 = 4$ (found by trial and error), which certainly satisfies $x_0^2 \equiv 5 \pmod{11}$. We then try $x = x_0 + 11k = 4 + 11k$, where we only care about k mod 11. Now $(4+11k)^2 = 16 + 88k + 11^2k^2 \equiv 16 + 88k \pmod{11^2}$, so we must solve the equation $16 + 88k \equiv 5 \pmod{11^2}$. Equivalently,

$$88k \equiv -11 \pmod{11^2} \iff 8k \equiv -1 \pmod{11} \iff k \equiv -7 \equiv 4 \pmod{11}.$$

(Note that the last step follows by noting that 7 is the inverse of 8 mod 11. This can be found by trial and error or by the Euclidean algorithm.) Anyhow we obtain $x = 4 + 11 \cdot 4 = 48$ as a solution. (Alternatively, if we start from $x_1 = 7$, we obtain another root $73 \pmod{11^2}$. Note that $73 \equiv -48 \pmod{11^2}$.)

4. Show that every number a has a unique cube root x modulo 101.

(For example, the number 14 has the cube root 6, since $6^3 = 216 \equiv 14 \pmod{101}$. I am asking you to show both existence and uniqueness of the cube root for any a, not just for 14.)

Answer. Note that 101 is a prime number. In case $a \equiv 0 \pmod{101}$, then the only solution is $x \equiv 0$. Otherwise, if $a \not\equiv 0 \pmod{101}$, then let g be a primitive root mod 101, and write $a \equiv g^b \pmod{101}$ for some b which is only determined modulo 100. We are looking for an $x \not\equiv 0 \pmod{101}$, so we can write $x \equiv g^y \pmod{101}$, where y is our "unknown" that is determined modulo 100. Then

$$x^3 \equiv a \pmod{101} \iff g^{3y} \equiv g^b \pmod{101} \iff 3y \equiv b \pmod{100}.$$

This last equation has a unique solution for y mod 100, since 3 is invertible modulo 100 [why?]. Once we know y, we then obtain a unique x.

5. Using the Chinese Remainder Theorem, find one solution x to the equation $x^2 \equiv 1 \pmod{91}$ with $x \not\equiv \pm 1 \pmod{91}$. (Again, you do not need to find the most general x of this form. It may help you to notice that $91 = 7 \cdot 13$.)

Answer. We want $x^2 \equiv 1$ modulo each of the primes 7 and 13, so by an argument from class we see that $x \equiv \pm 1$ modulo each of 7 or 13. To ensure that $x \not\equiv \pm 1 \pmod{91}$, we take a different choice modulo each prime:

$$x \equiv +1 \pmod{7}, \qquad x \equiv -1 \pmod{13}. \tag{$*$}$$

This can be solved by the Chinese Remainder Theorem. Explicitly, we see that $x = 13k-1$ but $x \equiv 1 \pmod{7}$, so we obtain $13k - 1 \equiv 1 \pmod{7}$, which we solve to obtain $k \equiv -2 \equiv 5 \pmod{7}$. This yields $x \equiv 13 \cdot 5 - 1 \equiv 64 \pmod{91}$. (One can alternatively solve the opposite system from $(*)$, and obtain the other solution $x \equiv 27 \pmod{91}$.)

6. Let p be a prime dividing $10^{32} + 1$. Show that $p \equiv 1 \pmod{64}$. Hint: what is the order of 10 modulo p?

Answer. We know that $10^{32} + 1 \equiv 0 \pmod{p}$, so we obtain $10^{32} \equiv -1 \pmod{p}$, and also $10^{64} \equiv (10^{32})^2 \equiv +1 \pmod{p}$. So the order of 10 modulo p is a factor of 64 but not a factor of 32, so the order of 10 is exactly 64. But we know by the little Fermat theorem that $10^{p-1} \equiv 1 \pmod{p}$, so the order of 10 is a factor of $p-1$. This implies $64 | p-1$, so $p \equiv 1 \pmod{64}$.

Note: $10^{32} + 1 = 19841 \cdot 976193 \cdot 6187457 \cdot 834427406578561$. Also note that we used implicitly the fact that $-1 \not\equiv 1 \pmod{p}$. This is okay, since $10^{32} + 1$ is odd, so $p \neq 2$.

7. In this question, p is a prime with $p \neq 2, 3$. Even if you cannot prove every part of this problem, you may assume the result of a previous part in all subsequent parts.

a) Show that $p \equiv \pm 1 \pmod{6}$.

b) Show that $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$.

c) Conclude that -3 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{6}$.

d) Show that there exist infinitely many primes of the form $6k + 1$.

Answer. a) p is odd, so $p \equiv 1$, 3, or $5 \pmod{6}$. But p is not divisible by 3, so the only choices are $p \equiv 1$ or $5 \pmod{6}$.

b) Case I: $p \equiv 1 \pmod{4}$, in which case $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (+1)\left(\frac{p}{3}\right)$.

Case II: $p \equiv 3 \pmod{4}$, in which case $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)(-\left(\frac{p}{3}\right)) = +\left(\frac{p}{3}\right)$.

c) -3 is a quadratic residue $\iff$ $\left(\frac{-3}{p}\right) = 1$ $\iff$ $\left(\frac{p}{3}\right) = 1$ $\iff$ $p \equiv 1 \pmod{3}$ $\iff$ $p \equiv 1 \pmod{6}$. The last equivalence is because the only choices of p modulo 6 are ± 1, and this determines the residue of p modulo 3.

d) Assume $p_1, p_2, \ldots, p_r$ are the **only** primes congruent to $1 \pmod{6}$. Form the number $N = 4(p_1 p_2 \cdots p_r)^2 + 3$. It is easy to see that N is not divisible by any of the primes $2, 3, p_1, p_2, \ldots, p_r$. So N is divisible by some other prime q. However, $N \equiv 0 \pmod{q}$ means that $4(p_1 p_2 \cdots p_r)^2 + 3 \equiv 0 \pmod{q}$, which means that the number $a = 2p_1 p_2 \cdots p_r$ satisfies $a^2 \equiv -3 \pmod{q}$. Thus by part (c), $q \equiv 1 \pmod{6}$, and we have located a new prime of the form $6k + 1$; contradiction. Thus there are infinitely many such primes.

Note: you can instead use the choice $N = 12(p_1 p_2 \cdots p_r)^2 + 1$. Do you see why?