Math 25, Test 2, November 12, 2008

Instructions. Show your work. Calculators are not permitted.

1. (15 pts.) Find two incongruent solutions to $x^3 \equiv 1 \pmod{169}$. (Note that $169 = 13^2$.)

   One solution is $x = 1$. To find a second, start with $x = 3$, which is a solution to $x^3 \equiv 1 \pmod{13}$. So take x of the form $3 + 13k$, which when cubed, we get $27 + 27 \cdot 13k \equiv 1 \pmod{169}$. Subtracting 1 and dividing through by 13, we get $2 + k \equiv 0 \pmod{13}$, so we can take $k = -2$, and $x = 3 - 2 \cdot 13 = -23$. (A third incongruent solution is $x = 22$ since the sum of the three cube roots of 1 mod 169 is 0 mod 169.)

2. (15 pts.) Calculate 3^{91} mod 1001 (the least nonnegative residue) by any valid method.

   One method is to write 91 in binary and go through the arithmetic we learned. This is fine if you like to do arithmetic. Here's a way if you don't. We know 1001 is the product of 7, 11, and 13. By Fermat, $3^6 \equiv 1 \pmod 7$, so that $3^{90} \equiv 1 \pmod 7$. Similarly, $3^{90} \equiv 1 \pmod{11}$. Now as you likely learned in problem 1, $3^3 \equiv 1 \pmod{13}$, so that $3^{90} \equiv 1 \pmod{13}$. Gluing these, we have $3^{90} \equiv 1 \pmod{1001}$, so the answer 3 is found by multiplying both sides by 3.

3. (10 pts.) Describe how the RSA cryptosystem is set up and used.

4. (10 pts.) Find all solutions to $\varphi(n) = n - 2$.

   Note that $n = 1, 2$ don't work. If $n > 2$, then $\varphi(n)$ is even, so if n is a solution to the equation, then n too is even. But an even number n has $\varphi(n) \le n/2$ (either see this from the formula, or note that the even numbers in $\{1, \ldots, n\}$ are not coprime to n). If a number that is at most $n/2$ is equal to $n - 2$, then n cannot be bigger than 4. So, $n = 4$ is the only candidate, and it works.

5. (15 pts.) Note that 1, 2, 3, 4 are four consecutive integers which are quadratic residues for 23. Find four consecutive integers which are quadratic residues for 29.

   One sees that $(2/29) = (3/29) = -1$, so that $(6/29) = 1$. Using the Law of Quadratic Reciprocity, we see too that $(5/29) = (7/29) = 1$, so that 4, 5, 6, 7 works. Another solution is 22, 23, 24, 25.

6. (10 pts.) The number $p = 2^{16} + 1 = 65{,}537$ is prime. Prove that an integer a is a primitive root for p if and only if it is a quadratic nonresidue for p.

   Suppose that a is a primitive root. It thus has order $p - 1$, so that $a^{(p-1)/2} \not\equiv 1 \pmod p$. Since this power is a square root of 1, it must be -1, so that by Euler's criterion, $(a/p) = -1$. Now suppose that $(a/p) = -1$, so that we have $a^{(p-1)/2} \equiv -1 \pmod p$. Then squaring both sides we see that the order of a divides $p - 1 = 2^{16}$, but does not divide $(p - 1)/2 = 2^{15}$. Thus, the order of a must be $2^{16} = p - 1$, so that a is a primitive root.

7. (15 pts.) A Carmichael number is a composite number n such that $a^{n-1} \equiv 1 \pmod{n}$ for all integers a coprime to n. Using what you know about congruences, prove that 1105 is a Carmichael number. (That is, do not use any “criterion” for Carmichael numbers, but rather principles from earlier in the course.)

   Factor 1105 as $5 \cdot 13 \cdot 17$. By Fermat’s little theorem, if a is coprime to 1105, we have $a^4 \equiv 1 \pmod{5}$, $a^{12} \equiv 1 \pmod{13}$, and $a^{16} \equiv 1 \pmod{17}$. Note that 4, 12, and 16 each divide 1104. Thus, $a^{1104} \equiv 1 \pmod{p}$ for $p = 5, 13, 17$, so it holds modulo 1105.

8. (10 pts.) Prove that if p is a prime and $p \equiv 3 \pmod{4}$, then for each integer a not divisible by p, exactly one of a and $-a$ is a quadratic residue for p.

   Since $p \equiv 3 \pmod{4}$, we have $(-1/p) = -1$, so that $(-a/p) = -(a/p)$. Since (a/p) is ± 1, one is 1 and the other is -1.

9. (10 bonus pts.) Show that $x^4 - x^2 + 1$ is reducible modulo every prime p.

   Rewrite as

$$\begin{aligned} x^4 - 2x^2 + 1 + x^2 &= (x^2 - 1)^2 + x^2, \\ x^4 + 2x^2 + 1 - 3x^2 &= (x^2 + 1)^2 - 3x^2, \\ x^4 - x^2 + 1/4 + 3/4 &= (x^2 - 1/2)^2 + 3/4. \end{aligned}$$

   Note that when $p \equiv 1 \pmod{4}$, the first rewrite can be factored modulo p as a difference of squares. When $p \equiv 11 \pmod{12}$, we have $(3/p) = 1$, so the second rewrite can be factored as a difference of squares. If $p \equiv 7 \pmod{12}$, then $(-3/p) = 1$, so the third rewrite can be factored as a difference of squares. Finally, modulo $p = 2$, the polynomial is the square of $x^2 + x + 1$.