Math 567, Assignment #4: Solutions

1. If k and n are relatively prime, there exist integers x and y such that $kx + ny = 1$, yielding $kx \equiv 1 \pmod{n}$. On the other hand, suppose k has a multiplicative inverse $x \pmod{n}$. Then $\gcd(k,n)|n|kx-1$ and $\gcd(k,n)|k|kx$, so $\gcd(k,n)|1$, implying $\gcd(k,n) = 1$.

2. $y^2 = x^2 - 15$ implies $15 = (x+y)(x-y)$; since x and y are integers, so are $x+y$ and $x-y$. Thus, to solve the equation in integers, we need to consider the ways of writing 15 as a product. If we assume that x and y are both positive, so is $x+y$; and since $x-y$ is the ratio of the two positive numbers 15 and $x+y$, $x-y$ must be positive too (but less than $x+y$). Thus the possible solutions to $y^2 = x^2 - 15$ in whole numbers correspond to the four ways of writing 15 as a product of two numbers, with the first greater than the second: $15 = 15 \times 1$ and $15 = 5 \times 3$. Solving $x + y = 15$, $x - y = 1$ yields $(x,y) = (8,7)$, and solving $x + y = 5$, $x - y = 3$ yields $(x,y) = (4,1)$. These are the only two solutions in positive integers; the general solution in integers is $(\pm 8, \pm 7),\ (\pm 4, \pm 1)$.

3. (a) We know that $3^{100} \equiv 1 \pmod{2}$ — that is, it's odd — so it suffices to find $3^{100} \bmod 5$. We know $3^4 \equiv 3^{5-1} \equiv 1 \pmod{5}$, so $3^{100} \equiv (3^4)^{25} \equiv 1^{25} \equiv 1 \pmod{5}$. Hence $3^{100} \equiv 1 \pmod{10}$. (In fact, it is congruent to 1 modulo 1000.)

(b) We know that $a^5 \equiv a \pmod{2}$, since there are just two cases to try ($a = 0$ and $a = 1$) and both work. Also, Fermat's theorem tells us that $a^5 \equiv a \pmod{5}$. Both congruences hold for all a. Hence the congruences hold modulo $\gcd(2,5) = 10$, which implies that a^5 and a have the same units digit.

4. (a) We compute $ax \equiv a(a^{p-2}b) \equiv a^{p-1}b \equiv 1b \equiv b \pmod{p}$.

(b) For the first congruence, we get $x \equiv 2^{29}1 \pmod{31}$; since $2^5 = 32 \equiv 1 \pmod{31}$, we have $2^{29} = (2^5)^5 2^4 \equiv 1^5 2^4 \equiv 16 \pmod{31}$. For the second congruence, we have $x \equiv 6^9 5 \equiv (6^3)^3 5 \equiv (216)^3 5 \equiv (7^3)5 \equiv (343)5 \equiv (2)5 \equiv 10 \pmod{11}$. For the third congruence, we have $x \equiv 3^{27}17 \equiv ((3^3)^3)^3 17 \equiv (27^3)^3 17 \equiv ((-2)^3)^3 17 \equiv (-8)^3 17 \equiv (-512)17 \equiv (-19)17 \equiv (10)17 \equiv 170 \equiv 25 \pmod{29}$.

This seems like a dumb way to solve linear congruences, but that's just because the numbers are so small; if the numbers involved were larger, this might well be a very efficient way to do it on a computer.

5. $1111 \equiv 5 \pmod 7$, so $2222 \equiv (2)(5) \equiv 3 \pmod 7$ and $5555 \equiv (5)(5) \equiv 4 \pmod 7$. Therefore $2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \pmod 7$. Since 7 is prime, Fermat's theorem tells us that 3^n and 4^n mod 7 depend only on n mod 6 $(= 7 - 1)$. Since $1111 \equiv 1 \pmod 6$, we have $5555 \equiv 5 \pmod 6$ and $2222 \equiv 2 \pmod 6$, so $3^{5555} + 4^{2222} \equiv 3^5 + 4^2 \pmod 7$. Thus we get $3^5 + 4^2 \equiv 243 + 16 = 259 \equiv 0 \pmod 7$.

6. (a) Suppose $p = 4k + 3$ is a prime dividing $n^2 + 1$. Then we get $p | n^2 + 1$, so that $n^2 \equiv -1 \pmod p$. This is a contradiction, since (by Theorem 5.5) -1 does not have a square root modulo any prime of the form $4k + 3$.

(b) Clearly the odd number $4N^2 + 1$ has only odd prime factors. Since $4N^2 + 1$ is of the form $n^2 + 1$, part (a) tells us that none of the primes dividing $4N^2 + 1$ can be of the form $4k + 3$. Hence all must be of the form $4k + 1$. Also note that no such prime can be a factor of N, since such a prime would divide both $4N^2 + 1$ and $4N$ and hence also divide their difference 1, which is impossible.

(c) Suppose there were only finitely many primes of the form $4k + 1$. Let N be the product of all such primes. Then by (b), $4N^2 + 1$ must have a prime factor of the form $4k + 1$ that is not on our list of all such primes.