Math 567, Assignment #5: Solutions

1. Suppose $p | 2^{32}+1$, so that $2^{32} \equiv -1 \pmod{p}$. Then we have $2^{64} \equiv (-1)^2 \equiv 1 \pmod{p}$, so that the order of 2 mod p must divide 64. However, the order of 2 mod p cannot be 32, or any divisor of 32, since $2^{32} \equiv -1 \not\equiv 1 \pmod{p}$. Hence the order of 2 mod p must be 64. Now, we also have $2^{p-1} \equiv 1 \pmod{p}$ (by Fermat's theorem), so 64 must divide $p-1$. That is, every prime divisor of $2^{32}+1$ must be congruent to 1 (mod 64). The first half-dozen primes of this kind are 193, 257, 449, 577, 641, and 769; it is not hard to check that $2^{32}+1$ (which equals 4294967297) is divisible by 641.

2. Suppose $p | 6^{16}+1$, so that $6^{16} \equiv -1 \pmod{p}$. Then we have $6^{32} \equiv (-1)^2 \equiv 1 \pmod{p}$, so that the order of 6 mod p must divide 32. However, the order of 6 mod p cannot be 16, or any divisor of 16, since $6^{16} \equiv -1 \not\equiv 1 \pmod{p}$. Hence the order of 6 mod p must be 32. Now, we also have $6^{p-1} \equiv 1 \pmod{p}$ (by Fermat's theorem), so 32 must divide $p-1$. That is, every prime divisor of $6^{16}+1$ must be congruent to 1 (mod 32). The first half-dozen primes of this kind are 97, 193, 257, 353, 449, and 577; it is not hard to check that $6^{16}+1$ (which equals 2821109907457) is divisible by 353.

3. (a) Setting aside the factors p and $2p$, we find that the factors (modulo p) are the numbers from 1 to $p-1$, taken twice; since (by Wilson's Theorem) $(p-1)! \equiv -1 \pmod{p}$, taking each of these factors twice gives us $(-1)^2 = 1 \pmod{p}$. If we include the factor $(p)(2p)/p^2 = 2$, we get $(2p)!/p^2 \equiv 2 \pmod{p}$.

(b) Setting aside the factors p, $2p$, and $3p$, we find that the factors (modulo p) are the numbers from 1 to $p-1$, taken three times, which gives us $(-1)^3 = -1 \pmod{p}$. If we include the factor $(p)(2p)(3p)/p^3 = 6$, we get $(3p)!/p^3 \equiv -6 \equiv p-6 \pmod{p}$.

(c) If p is odd, the factors of $(p^2)!$ that aren't multiples of p contain each of the residues from 1 to $p-1$ exactly p times, giving the product $(-1)^p \pmod{p}$. The remaining factors p, $2p$, $3p$, …, p^2 involve $p+1$ factors of p, and when these factors are removed, we are left with $1 \times 2 \times 3 \times \ldots \times (p-1)$, which is just $(p-1)!$. Using Wilson's Theorem one last time, we get the product $(-1)^p(-1) = (-1)^{p+1} = 1$ (since p is odd). When p is even (i.e., $p = 2$) we can verify directly that $(p^2)!/p^{p+1}$ is $1 \pmod{p}$. Hence the result holds for all primes p.

(d) Let x denote the value of this product modulo p. x is a product of $(p-1)/2$ residues modulo p; the remaining residues are precisely the negatives of the ones that occur in x. Hence the product of these other $(p-1)/2$ residues is $(-1)^{(p-1)/2}x$. Multiplying these two products together and applying Wilson's Theorem, we get $(-1)^{(p-1)/2}x^2 \equiv -1 \pmod{p}$. Hence $x^2 \equiv (-1)^{(p+1)/2}$, which is 1 or -1 according to whether p is 3 mod 4 or 1 mod 4.

4. (a) f is not multiplicative. E.g., $f(2) = 2$ and $f(3) = 3$ but $f(6) = 2+3 = 5 \neq 6 = f(2)f(3)$.

(b) g is multiplicative. One slick way to see this is to introduce the function $g'(n)$ which equals n if n is a perfect square and 0 otherwise. Since $g(n) = \sum_{d|n} g'(d)$, Theorem 6.4 assures us that g must be multiplicative if g' is. To prove the multiplicativity, we need only show that the product of two relatively prime numbers is a perfect square if and only if the two numbers are squares separately. One direction is easy: a product of two squares is always a square. To prove the other direction, suppose ab is a square with $\gcd(a, b) = 1$. Write $a = \prod p_i^{e_i}$ and $b = \prod p_i^{f_i}$, where $p_1, p_2, p_3, \ldots$ are the primes. The condition $\gcd(a, b) = 1$ implies that for all i, $\min(e_i, f_i) = 0$. The condition that ab is a square implies that $e_i + f_i$ is even for all i. Combining these two conditions on the exponents e_i and f_i, we see that for all i, *both* e_i and f_i are even; hence a and b are perfect squares, as claimed.

(c) h is multiplicative. Suppose m, n are relatively prime with $h(m) = A$, $h(n) = B$. Write the A solutions of $x^2 \equiv -1 \pmod{m}$ as $x_1, ..., x_A$ and the B solutions of $x^2 \equiv -1 \pmod{n}$ as $y_1, ..., y_B$. For any x_i and y_j, the Chinese Remainder Theorem gives us a value $z_{i,j}$ with $z_{i,j} \equiv x_i \pmod{m}$ and $z_{i,j} \equiv y_j \pmod{n}$, from which it follows that $z_{i,j}^2 \equiv -1 \pmod{mn}$. (Some steps to fill in: We have $z_{i,j}^2 \equiv -1 \pmod{m}$, so $z_{i,j}^2 + 1$ is divisible by m. Likewise it is divisible by n. Since m, n are relatively prime, $z_{i,j}^2 + 1$ is divisible by mn.) Moreover, every solution to $z^2 \equiv -1 \pmod{mn}$ arises in this way exactly once, namely from the unique pair x_i, y_j such that $z \equiv x_i \pmod{m}$ and $z \equiv y_j \pmod{n}$. Hence the number of solutions to $z^2 \equiv -1 \pmod{mn}$ is AB, as desired.