Geoffrey Thomas 18.781 problem set 3 Collaborators: Liz Denys and Yuri Lin

2.2 8 Any solution must satisfy $x^2 \equiv 1 \mod p$, i.e., $x = kp + 1$ or $x = kp - 1$. In the original congruence, this would mean $k^2p^2 \pm 2kp + 1 \equiv 1 \mod p^\alpha$, or $kp(kp \pm 2) \equiv 0 \mod p^\alpha$. So the solutions are $k = 0$, i.e., $x = \pm 1$, or $kp \equiv \pm 2 \mod p^\alpha$. Since p is prime, k is unique, and we know at least one k that satisfies this, namely $\pm 2p^{\alpha-1}$. But then x is, again, ± 1.

2.2 14 Consider the power of p in the numerator and denominator. The binomial coefficient is

$$\frac{p^\alpha(p^\alpha - 1)\cdots(p^\alpha - k + 1)}{k(k-1)\cdots 1}$$

with the same number of terms on the numerator and denominator. Note that $p^\alpha \equiv 0 \mod p$. Given that, and that multiples of p occur every p integers, there is at least one more multiple of p on the top than on the bottom, counting the bottom upwards from 1 and the top downwards from p^α. Similarly, there is one more multiple of p^2, one more of p^3, etc., up to p^α, of which there is one more multiple (it exists on the top and not on the bottom). Therefore, the power of p in the numerator is higher than that in the denominator, and so the binomial coefficient is a multiple of p, i.e., congruent to $0 \mod p$.

2.3 9 $\phi(1) = 1$ and $\phi(2) = 1$. Consider any power of two 2^n where $n > 1$. Its totient is $2^n\left(1 - \frac{1}{2}\right) = 2^{n-1}$, which is even. Now consider any odd prime power p^n. Its totient is $p^n\left(1 - \frac{1}{p}\right) = (p-1)\,p^{n-1}$, which is even because $p - 1$ is even. Now consider any composite number. Its totient is the product of its factors' totients, and so since it can be expressed in product-of-powers-of-primes form, its totient is only not even if it contains no powers of two beyond 2, and no nonzero powers of any other primes. This is only true for 1 2.

2.3 17 $143 = 11\times 13$, so we have the two congruences $(x-1)(x-3)(x-5) \equiv 0 \mod 11$ and $(x-1)(x-3)(x-5) \equiv 0 \mod 13$. The original congruence is true if both are true. The solutions to the first are $1, 3, 5 \mod 11$ and to the second $1, 3, 5 \mod 13$, so were are looking for all numbers modulo 143 that are equivalent to one of the solutions in each set. Since 11 and 13 are relatively prime, we have exactly one residue modulo 143 that is equivalent to one number from each solution set, by the Chinese Remainder Theorem. So our solutions are 1, 143, 122, 14, 3, 135, 27, 16, and 5.

2.3 23

2.3 24

2.3 29 Should $(2, n) = 1$, then $\phi(2n) = \phi(2)\phi(n) = \phi(n)$. If not, then note that in the representation $\phi n = n\prod_{p_n}\left(1 - \frac{1}{p}\right)$, that replacing n with $2n$ does not affect the product, since $2|n$ and $2|2n$, but it does affect the coefficient on the product, so $\phi 2n = 2\phi n$. So for all odd integers $\phi 2n = \phi n$, and for all even integers, $\phi 2n = 2\phi n$.

2.5 2 We can expand $\phi = pq - p - q + 1 = m - p - q + 1$, and then substitute $q = m/p$ to yield $\phi = m - p - m/p + 1$, or $p\phi = mp - p^2 - m + p$. This can be solved with the quadratic formula, and since we could as easily have substituted p, the two solutions are the two values of p and q.

By applying the quadratic formula we find that m factors into 9839 and 3989.

5a Every binomial coefficient other than $\binom{p^k}{0}$ and $\binom{p^k}{p^k}$ will have p^k as a factor, by 2.2 14, and the right side of the congruence is just the first and last terms. So the difference is divisible by p^k, which demonstrates the identity.

6 This holds if n is prime; by the same reasoning as 5a, every term on the left except the first and last is divisible by n, leaving $a^n \equiv a \mod n$, which we know is true for every integer if n is prime.