Homework #1

Problems to hand in on Thursday, January 24, in the beginning of class. Write your answers out carefully, staple pages, and write your name and section number on each page.

1) In this problem, we will give two proofs of the following FACT:

"*If n is an odd integer, the remainder of n^2 when divided by* 8 *is* 1."

(a) First, prove the FACT directly by writing $n = 2k + 1$ using the division algorithm and "FOIL"ing.

(b) Second, show that n is congruent to either $1, 3, 5$, or 7 modulo 8. Show that if the FACT is true when $n = 1, 3, 5$, or 7, then it holds for every odd integer, and complete the proof.

Solution.

(a) By the Division Algorithm, we can write $n = 2k+1$ for some integer k. Then $(2k+1)^2 = 4k^2 + 4k + 1$.
When $k \equiv 1 \mod 8$, $4k^2 + 4k + 1 \equiv 4 + 4 + 1 \equiv 1 \mod 8$.
When $k \equiv 2 \mod 8$, $4k^2 + 4k + 1 \equiv 0 + 0 + 1 \equiv 1 \mod 8$.
When $k \equiv 3 \mod 8$, $4k^2 + 4k + 1 \equiv 4 * 9 + 12 + 1 \equiv 1 \mod 8$.
when $k \equiv 4 \mod 8$, $4k^2 + 4k + 1 \equiv 0 + 0 + 1 \equiv 1 \mod 8$.

(b) Any integer is congruent to some number between 0 and 7 mod 8. Elements of the congruence classes of $0, 2, 4, 6$ are even, so n must congruent to one of $1, 3, 5, 7$. Now, if $n \equiv m \mod 8$, then $n^2 \equiv m^2 \mod 8$, so it suffices to show that the fact holds for $1, 3, 5$ and 7. We check these individually: their squares are $1, 9, 25, 49$, which are all congruent to one modulo 8.

2) Show that if p is a prime integer *other than* ± 2 *or* ± 3, then $p^2 - 1$ is a multiple of 24.

Solution. Any such prime is odd, so $8|(p^2 - 1)$ by the previous problem. Additionally, one of the three consecutive numbers $p-1$, p, and $p+1$ is a multiple of three; since p is a prime other than three, it must be either $p-1$ or $p+1$. It follows that $3|(p-1)(p+1) = (p^2 - 1)$.

Now, the prime factorization of $p^2 - 1$ must contain the prime 2 with multiplicity three (since 8 divides it), and must also contain the prime 3 (since 3 divides it). It follows that $24|(p^2 - 1)$.

3) Let $f(x)$ and $g(x)$ be two polynomials with integer coefficients. We say that f *is a factor of* g *in the ring* $\mathbb{Z}[x]$ if there is another polynomial with integer coefficients, $h(x)$, such that $g = fh$.

(a) Show that, for any n, $f(x) = x - 1$ is a factor of $g(x) = x^n - 1$ in the ring $\mathbb{Z}[x]$.

(b) Use this to show that any power of 10, $100 \cdots 00$, is congruent to 1 modulo 9.

(c) Use this to show that any positive integer is congruent to the sum of its digits modulo 9.

(d) Now show that if $a = 100\cdots00$ has an *even* number of zeroes, then $a \equiv 1 \bmod 11$, and if $a = 100\cdots00$ has an *odd* number of zeroes, then $a \equiv -1 \mod 11$.

(e) Show that any positive integer n is congruent to

$$(\text{unit digit of } n) - (\text{tens digit of } n) + (\text{hundreds digit of } n) - \cdots \pm \cdots$$

modulo 11.

Solution.

(a) $(1 + x + x^2 + \cdots + x^{n-1})(x - 1) = x^n - 1$.

(b) Plugging in $x = 10$ to part (a), we get $(10 - 1)|(10^n - 1)$ for any n. This means that 10^n is congruent to 1 modulo 9.

(c) Write out a positive integer in terms of its decimal expansion $n = a_d a_{d-1} \cdots a_1 a_0$, where a_i is the digit in the i-th place. This means $n = a_d \times 10^d + a_{d-1} \times 10^{d-1} + \cdots + a_1 \times 10^1 + a_0$. Using the previous part, we then have

$$\begin{aligned} n &= a_d \times 10^d + a_{d-1} \times 10^{d-1} + \cdots + a_1 \times 10^1 + a_0 \\ &\equiv a_d \times 1 + a_{d-1} \times 1 + \cdots + a_1 \times 1 + a_0 \mod 10, \end{aligned}$$

which is what we wanted to show!

(d) Plug in $x = -10$ to part (a). We get that $(-10 - 1)|((-10)^n - 1)$. If n is even (even number of zeroes), then we get $-11|10^n - 1$, so $10^n \equiv 1 \bmod 11$. If n is odd (odd number of zeroes), then $-11| - 10^n - 1$, so $11|10^n + 1$, so $10^n \equiv -1 \mod 11$.

(e) Write out the decimal expansion of n as in part (c). Using part (d), we have

$$\begin{aligned} n &= a_d \times 10^d + a_{d-1} \times 10^{d-1} + \cdots + a_1 \times 10^1 + a_0 \\ &\equiv a_d \times (-1)^d + a_{d-1} \times (-1)^{d-1} + \cdots + a_1 \times -1 + a_0 \mod 10, \end{aligned}$$

which is equivalent to the expression in the statement.

4) For any integer m, we can use the Fundamental Theorem of Arithmetic to write $m = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ where the p_i's are distinct primes in an (essentially) unique way. The natural number a_i is said to be the multiplicity of the prime p_i in m. [By convention, the multiplicity of p in m is 0 if p does not divide m.]

(a) Let d and n be positive integers. Prove that n is a d-th power of some other integer if and only if for every prime p, the multiplicity of p in n is divisible by d.

(b) Prove that if n is not a d-th power of some other integer, then $\sqrt[d]{n}$ is irrational. [Hint: try proof by contradiction.]

Solution.

(a) Suppose that n is the d-th power of some integer m. Write $m = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ as above. Then, $n = m^d = p_1^{da_1} p_2^{da_2} \cdots p_t^{da_t}$, so the multiplicities of the primes are all multiples of d.

Now suppose that the multiplicity of each prime in n is a multiple of d. We can then write $n = p_1^{da_1} p_2^{da_2} \cdots p_t^{da_t}$, and setting $m = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$, we obtain that $n = m^d$, so it is a d-th power.

(b) We will prove the contrapositive. Assume that $\sqrt[d]{n}$ is rational. We can then write $\sqrt[d]{n} = a/b$ for some integers a, b. Raising both sides to the power d, we get $n = a^d/b^d$, so $nb^d = a^d$. Write $e_p(k)$ for the multiplicity of the prime p in the integer k. We know that for any prime p, that $e_p(n) + e_p(b^d) = e_p(a^d)$, and that $d|e_p(b^d)$ and $d|e_p(a^d)$ from the previous part. It follows that for any prime p that $d|e_p(n)$. But, again by the previous part, this means that n is a d-th power of some other integer.

5) Let n and d be non-negative integers. The notation $\binom{n}{m}$ denotes the quantity $\frac{n!}{m!(n-m)!}$. [By convention, we define $0! = 1$.]

(a) Show that for all $1 \leqslant d < n$, $\binom{n}{d} = \binom{n-1}{d} + \binom{n-1}{d-1}$.

(b) Use the previous part to show that $\binom{n}{d}$ is an integer for any $0 \leqslant d \leqslant n$.

(c) Use the fundamental theorem of arithmetic to show that if p is prime and $1 \leqslant d < p$, then $p| \binom{p}{d}$.

Solution.

(a)

$$\begin{aligned}
\binom{n-1}{d} + \binom{n-1}{d-1} &= \frac{(n-1)!}{(n-1-d)!d!} + \frac{(n-1)!}{(n-1-(d-1))!(d-1)!} \\
&= \frac{(n-1)!}{(n-1-d)!d!} + \frac{(n-1)!}{(n-d)!(d-1)!} \\
&= \frac{(n-1)! \cdot (n-1-d)}{(n-d)!d!} + \frac{(n-1)! \cdot d}{(n-d))!d!} \\
&= \frac{(n-1)! \cdot ((n-d)+d)}{(n-d))!d!} \\
&= \frac{(n-1)! \cdot n}{(n-d))!d!} \\
&= \binom{n}{d}.
\end{aligned}$$

(b) First, note that for any n, $\binom{n}{0} = \frac{n!}{n!0!} = 1$ is also an integer, and so is $\binom{n}{n} = \frac{n!}{n!0!} = 1$. We will use induction on n; note that by our conditions, our statement is about $n \geqslant 2$. When $n = 2$, the only d that remains is $d = 1$; $\binom{2}{1} = \frac{2!}{1!1!} = 2$, which is an integer. Now suppose that we have a fixed value of $n \geqslant 2$ for which we have already shown $\binom{n}{d}$ us an integer for all $0 \leqslant d \leqslant n$. Now consider $n+1$, and fix any $0 \leqslant d \leqslant n+1$.We have

already done the cases $d = 0$ and $d = n+1$, so we might as well assume $1 \leqslant d < n+1$. By part (a),

$$\binom{n+1}{d} = \binom{n}{d} + \binom{n}{d-1}$$

By induction hypothesis, $\binom{n}{d}$ and $\binom{n}{d-1}$ are both integers; their sum must also be an integer.

(c) We have shown that $\binom{p}{d}$ is an integer. On the other hand, $\binom{p}{d} = \frac{p!}{d!(p-d)!}$. By the Fundamental Theorem of Arithmetic, we can write $p! = q_1 \cdots q_s$ as a product of primes, and p appears as one of the q_i's. We observe that $d!$ and $(n-d)!$ are products of integers that are all smaller than p. Each of the prime factors of these terms must be smaller than p, so p cannot be a prime factor of either $d!$ or $(n-d)!$. Now, $p|p! = \binom{p}{d} \cdot d! \cdot (n-d)!$. By a property of primes from the worksheet, we must have that $p|\binom{p}{d}$.