Homework 2

Aleck Zhao

September 17, 2016

Section 1.1: Induction

14. (a) Show that

$$\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n}=2^n$$

for all $n \geq 0$.

Proof. We proceed by induction. The base case is $n=0$. In this case, $\binom{0}{0}=1=2^0$ thus the statement is true for $n=0$.

Next, assume that the hypothesis is true for arbitrary $k \in \mathbb{N}$, so that

$$2^k=\sum_{i=0}^{k}\binom{k}{i}.$$

Consider the sums

$$\begin{aligned} S_{k+1}&=\sum_{i=0}^{k+1}\binom{k+1}{i}=\binom{k+1}{0}+\binom{k+1}{1}+\cdots+\binom{k+1}{k}+\binom{k+1}{k+1}\\ S_k&=\sum_{i=0}^{k}\binom{k+0}{i}=\binom{k+0}{0}+\binom{k+0}{1}+\cdots+\binom{k+0}{k}\end{aligned}$$

Then

$$S_{k+1}-S_k=\binom{k+1}{k+1}+\binom{k+1}{0}-\binom{k}{0}+\sum_{i=1}^{k}\left[\binom{k+1}{i}-\binom{k}{i}\right]$$

where the summand can be simplified as

$$\begin{aligned}\binom{k+1}{i}-\binom{k}{i}&=\frac{(k+1)!}{i!(k+1-i)!}-\frac{k!}{i!(k-i)!}\\ &=\frac{k!}{i!(k-i)!}\left(\frac{k+1}{k+1-i}-1\right)\\ &=\frac{k!}{i!(k-i)!}\cdot\frac{i}{k+1-i}\\ &=\frac{k!}{(i-1)!(k+1-i)!}\\ &=\binom{k}{i-1}\end{aligned}$$

Thus,

$$\begin{aligned} S_{k+1} - S_k &= \binom{k+1}{k+1} + \sum_{i=1}^{k} \binom{k}{i-1} \\ &= \binom{k}{k} + \sum_{j=0}^{k-1} \binom{k}{j} \\ &= \sum_{j=0}^{k} \binom{k}{j} \\ &= 2^k. \end{aligned}$$

Thus, $S_{k+1} = S_k + 2^k = 2^k + 2^k = 2^{k+1}$, so the hypothesis is true for $k+1$, completing the proof.

□

(b) Show that

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots \pm \binom{n}{n} = 0$$

if $n > 0$.

Proof. We proceed by induction. The base case is $n = 1$. In this case, $\binom{1}{0} - \binom{1}{1} = 0$ thus the statement is true for $n = 1$.

Next, assume the hypothesis is true for arbitrary $k \in \mathbb{N}$, so that

$$0 = \sum_{i=1}^{k} (-1)^i \binom{k}{i}.$$

Consider the sums

$$\begin{aligned} S_{k+1} &= \sum_{i=0}^{k+1} (-1)^i \binom{k+1}{i} = \binom{k+1}{0} - \binom{k+1}{1} + \cdots \pm \binom{k+1}{k} \mp \binom{k+1}{k+1} \\ S_k &= \sum_{i=0}^{k} (-1)^i \binom{k+0}{i} = \binom{k+0}{0} - \binom{k+0}{1} + \cdots \pm \binom{k+0}{k} \end{aligned}$$

Then

$$\begin{aligned} S_{k+1} - S_k &= \mp \binom{k+1}{k+1} + \sum_{i=1}^{k} (-1)^i \binom{k}{i-1} \\ &= \mp \binom{k}{k} - \sum_{j=0}^{k-1} (-1)^j \binom{k}{j} \\ &= - \left(\sum_{j=0}^{k} (-1)^j \binom{k}{j} \right) \\ &= 0 \end{aligned}$$

so $S_{k+1} = S_k = 0$, completing the proof.

□

18. (b) Conjecture a formula for a_n and prove it by induction:

$$a_0 = 1, a_1 = -2, a_{n+2} = 2a_n - a_{n+1}, n \geq 0.$$

Conjecture 0.1. We claim that a_n is given by the closed form

$$a_n = 4 - 3 \cdot 2^n$$

for all $n \geq 0$.

Proof. We proceed by strong induction. The base cases are $n = 0, 1$. We have

$$\begin{aligned} a_0 &= 1 = 4 - 3 \cdot 2^0 \\ a_1 &= -2 = 4 - 3 \cdot 2^1 \end{aligned}$$

so the hypothesis is true for the base cases.
Next we assume that $a_k = 4 - 3 \cdot 2^k$ for all $1 \leq k \leq m+1$. Thus

$$\begin{aligned} a_m &= 4 - 3 \cdot 2^m \\ a_{m+1} &= 4 - 3 \cdot 2^{m+1} \end{aligned}$$

so that

$$\begin{aligned} a_{m+2} = 2a_m - a_{m+1} &= 2(4 - 3 \cdot 2^m) - (4 - 3 \cdot 2^{m+1}) \\ &= (8 - 3 \cdot 2^{m+1}) - (4 - 3 \cdot 2^{m+1}) \\ &= 4 - 6 \cdot 2^{m+1} \\ &= 4 - 3 \cdot 2^{m+2} \end{aligned}$$

which is exactly the closed form in the conjecture, thus proven.

□

Section 1.2: Divisors and Prime Factorization

18. If $\gcd(m, n) = 1$, let $d = \gcd(m+n, m-n)$. Show that $d = 1$ or $d = 2$.

Proof. Since $d|m+n$ and $d|m-n$, it follows that

$$\begin{aligned} d|[(m+n) + (m-n)] &\implies d|2m \\ d|[(m+n) - (m-n)] &\implies d|2n \end{aligned}$$

Let $h = \gcd(2m, 2n)$. Since d divides both $2m$ and $2n$, it follows that d must divide their gcd, h. But since $\gcd(m, n) = 1 \implies \gcd(2m, 2n) = 2$, the fact that d must divide h means that d must divide 2, so $d = 1$ or $d = 2$, as desired.

□

22. If $d_1, \cdots, d_r$ are divisors of n and if $\gcd(d_i, d_j) = 1$ whenever $i \neq j$, show that $d_1 d_2 \cdots d_r$ divides n.

Proof. By Theorem 5, if d_1 and d_2 are relatively prime and $d_1|n$ and $d_2|n$, then their product $d_1 d_2|n$. Next, since d_3 is relatively prime to d_1 and d_2, then d_3 is relatively prime to the product $d_1 d_2$. Thus since $d_3|n$ and $d_1 d_2|n$, it follows that $d_1 d_2 d_3|n$. Continuing in this fashion, we conclude that $d_1 d_2 \cdot d_r|n$, as desired.

□

38. If q is a rational number such that q^2 is an integer, show that q is an integer.

Proof. Since q is rational, we may write $q = \frac{m}{n}$ for $m, n \in \mathbb{Z}$. Thus $q^2 = \frac{m^2}{n^2} \in \mathbb{Z}$, so it must be that $n^2|m^2$. Let the prime factorization of m be

$$m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where p_i are distinct primes and $e_i \geq 1$. Then the prime factorization of m^2 is

$$m^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k}.$$

By Theorem 8, all divisors d of m^2 are of the form

$$d = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$$

where $1 \leq d_i \leq 2e_i$ for all $1 \leq i \leq k$. Since n^2 divides m^2, it too has this form, and since it is the square of an integer, its exponents must all be even. Thus write

$$n^2 = p_1^{2f_1} p_2^{2f_2} \cdots p_k^{2f_k}$$

where $1 \leq 2f_i \leq 2e_i$ for all i. Then taking the square root, we have

$$n = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}.$$

Since $2f_i \leq 2e_i$, it follows that $f_i \leq e_i$, so then n must divide m by Theorem 8, so $q = \frac{m}{n}$ is an integer, as desired.

□

42. Show that $\gcd(a, b, c) = \gcd[a, \gcd(b, c)]$.

Lemma 0.2

For any integers $x, y, z \in \mathbb{Z}$, we have

$$\max(x, y, z) = \max(x, \max(y, z)).$$

Proof. We have 3 cases, one where each of x, y, z is the maximum of the three.

Case 1: x is maximum. Then $\max(y, z) \leq x$, so

$$\max(x, \max(y, z)) = x = \max(x, y, z).$$

Case 2: y is maximum. Then $\max(y, z) = y \geq x$, so

$$\max(x, \max(y, z)) = \max(x, y) = y = \max(x, y, z).$$

Case 3: z is maximum. This is identical to Case 2.

Thus

$$\max(x.y.z) = \max(x, \max(y, z)),$$

as desired. □

Proof. WLOG all of a, b, c are positive, since negative numbers only differ by a factor of -1. Let p_k be the greatest prime that divides any of a, b, c. Then we may write factorizations of a, b, c as

$$\begin{aligned} a &= p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \\ b &= p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \\ c &= p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k} \end{aligned}$$

where p_i are all primes ranging from 2 to p_k, and e_i, f_i, g_i are all non-negative integers, where they are 0 if a, b, c are not divisible by p_i, respectively. Then, by Theorem 9, we have

$$\gcd(a, b, c) = \prod_{i=1}^{k} p_i^{\max(e_i, f_i, g_i)}.$$

We also have

$$\gcd(b, c) = \prod_{i=1}^{k} p_i^{\max(f_i, g_i)}$$

and then

$$\begin{aligned} \gcd[a, \gcd(b, c)] &= \gcd\left(a, \prod_{i=1}^{k} p_i^{\max(f_i, g_i)}\right) \\ &= \gcd\left(\prod_{i=1}^{k} p_i^{e_i}, \prod_{i=1}^{k} p_i^{\max(f_i, g_i)}\right) \\ &= \prod_{i=1}^{k} p_i^{\max(e_i, \max(f_i, g_i))} \\ &= \prod_{i=1}^{k} p_i^{\max(e_i, f_i, g_i)} \end{aligned}$$

where the last step is due to Lemma 0.2. Thus

$$\gcd(a, b, c) = \gcd(a, \gcd(b, c))$$

as desired.

$\square$

Section 1.3: Integers Modulo n

8. (b) Find the remainder when 8^{391} is divided by 5.

Solution. By Fermat's Little Theorem, we have $8^4 \equiv 1 \pmod 5$. Then $8^{388} \equiv (8^4)^{97} \equiv 1^{97} \equiv 1 \pmod 5$. Finally $8^{391} \equiv 8^3 \cdot (8^4)^{97} \equiv 8^3 \cdot 1 \equiv 512 \equiv \boxed{2 \pmod 5.}$

$\square$

21. (b) Let $n = d_k d_{k-1} \cdots d_2 d_1 d_0$ be the decimal representation of n. Show that $11|n$ if and only if 11 divides $(d_0 - d_1 + d_2 - d_3 + \cdots \pm d_k)$.

Proof. Rewrite n as

$$n = 10^k d_k + 10^{k-1} d_{k-1} + \cdots + 10^2 d_2 + 10^1 d_1 + 10^0 d_0.$$

We have $10 \equiv -1 \pmod{11}$, which means $10^k \equiv -1 \pmod{11}$ for odd k and $10^k \equiv 1 \pmod{11}$ for even k. Then taking $n \pmod{11}$, we have

$$\begin{aligned} n \pmod{11} &\equiv 10^0 d_0 + 10^1 d_1 + \cdots + 10^k d_k \pmod{11} \\ &\equiv d_0 - d_2 + \cdots \pm d_k \pmod{11} \end{aligned}$$

where the sign of d_k depends on if k is even or odd.

If $11|n$, then $n \in [0]_{11}$ and since $n \equiv (d_0 - d_1 + \cdots \pm d_k) \pmod{11}$ it follows that $(d_0 - d_1 + \cdots \pm d_k) \in [0]_{11}$ as well, so $11|(d_0 - d_1 + \cdots \pm d_k)$, as desired. The converse follows similarly.

□

28. Find $x \in \mathbb{Z}$ such that $x \equiv 8 \pmod{10}, x \equiv 3 \pmod{9}, x \equiv 2 \pmod{7}$.

Solution. By the Euclidean Algorithm, we have

$$\begin{aligned} 9 &= 1(7) + 2 \\ 7 &= 3(2) + 1 \end{aligned}$$

so we may write

$$\begin{aligned} 1 &= 7 - 3(2) \\ &= 7 - 3(9 - 7) \\ &= 4 \cdot 7 - 3 \cdot 9. \end{aligned}$$

Then

$$x \equiv 3(4 \cdot 7) - 2(3 \cdot 9) \pmod{7 \cdot 9} \equiv 30 \pmod{63}$$

is a class of solutions to the two equivalences $x \equiv 3 \pmod{9}$ and $x \equiv 2 \pmod{7}$ since 7 and 9 are relatively prime.

Next, using the Euclidean Algorithm between 63 and 10, we have

$$\begin{aligned} 63 &= 6(10) + 3 \\ 10 &= 3(3) + 1 \end{aligned}$$

so we may write

$$\begin{aligned} 1 &= 10 - 3(3) \\ &= 10 - 3(63 - 6(10)) \\ &= 19 \cdot 10 - 3 \cdot 63. \end{aligned}$$

Then

$$\begin{aligned} x &\equiv 30(19 \cdot 10) - 8(3 \cdot 63) \pmod{10 \cdot 63} \\ &\equiv 4188 \pmod{630} \\ &\equiv \boxed{408 \pmod{630}} \end{aligned}$$

is a class of solutions to all three equivalences simultaneously. □

31. Show that the following conditions on an integer $n \geq 2$ are equivalent.

(1) If $\bar{a} \in \mathbb{Z}_n$, then either $\bar{a}$ is invertible or $\bar{a}^k = \bar{0}$ for some $k \geq 1$.

(2) n is a power of a prime.

Proof. We need to prove both (1) $\implies$ (2) and (2) $\implies$ (1).

Assume (2). If n is a power of a prime, write $n = p^i$ for $i > 1$. If $\bar{a}$ and n are not relatively prime, then it must be that $\bar{a}$ is of the form bp^j for some $b \in \mathbb{Z}$ and $j > 1$. Then $\bar{a}^i = (bp^j)^i = b^i(p^i)^j = b^i \cdot \bar{0}^j = \bar{0}$. On the other hand, if $\gcd(\bar{a}, n) = 1$, by Theorem 5, $\bar{a}$ has an inverse in $\mathbb{Z}_n$, as desired.

Assume (1). Then for all $\bar{a} \in \mathbb{Z}_n$, either $\bar{a}$ is invertible or $\bar{a}^k = \bar{0}$ for some $k \geq 1$. Let n be of the form bp^i where p is some prime that divides n, and b is a nonzero integer that is not divisible by p. Consider $\bar{a} = b$. Assume that $\gcd(b, bp^i) = b \neq 1$. Then b does not have an inverse in $\mathbb{Z}_n$. However, since $\gcd(b, p) = 1$, it follows that $\gcd(b^k, p^i) = 1$ as well, so bp^i will never divide b^k for any k. Thus $b^k \neq \bar{0}$, which contradicts our assumption of (1). Thus, $\gcd(b, bp^i) = b = 1$, thus $n = bp^i = p^i$ is a power of a prime, as desired.

□