ch 5

(#15) $x^3 \equiv 1 \bmod 2 \Rightarrow x^3 = 1$ in $\mathbb{Z}_2 = \{0,1\}$

$\Rightarrow x = 1$ in $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$

$\Rightarrow x \equiv 1 \bmod 2$

$\Rightarrow x - 1 = 2k$

$\Rightarrow x = 2k+1$

(17) $n = 2k+1 \Rightarrow n^2 - 1 = 4k^2 + 4k + x - x$

$= 4k(k+1)$

$\exists$ k or $k+1$ $\equiv \bmod 2$

(18) $(a+b)^3 = a^3 + b^3 \bmod 3$

(20) $a \in \mathbb{Z}$ $\nexists$ $a \equiv 1 \bmod 5 \Rightarrow a^2 \equiv 1 \bmod 5$

i.e. $a = 1 \in \mathbb{Z}_5 \Rightarrow a^2 = 1 \in \mathbb{Z}_5$

pf: $a = 1 \in \mathbb{Z}_5 \Rightarrow a - 1 = 5k$

$\Rightarrow a^2 - 1 = (a-1)(a+1)$

$= 5k(a+1)$

$\Rightarrow a^2 \equiv 1 \bmod 5$

(21) $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. Then

$$a \equiv b \bmod n \implies a^3 \equiv b^3 \bmod n$$

i.e. $a = b \in \mathbb{Z}_n \implies a^3 \equiv b^3 \in \mathbb{Z}_n$

pf: $a \equiv b \bmod n$

$$\implies a - b = kn$$

$$\implies a^3 - b^3 = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$$

$$= kn(\ \text{“}\ \text{”}\ )$$

$$\implies a^3 \equiv b^3 \bmod n \text{ or } a^3 \equiv b^3 \text{ in } \mathbb{Z}_n$$

(24) $a \equiv b \bmod n$, $c \equiv d \bmod n$

$$\implies ac \equiv bd \bmod n$$

pf: $a - b = kn$, $c - d = ln \implies a = kn + b$

$$c = ln + d$$

$$\implies ac - bd = (kn+b)(ln+d) - bd$$

$$= (kln)n + (kd + bl)n + bd - bd$$

$$= (kln + kd + bl)n$$

$$\implies ac \equiv bd \bmod n$$

(26) If $k \in \mathbb{N}$ (i.e. $k \geq 1$, according to Hammack, p. 4) and $n = 2^k - 1$, then every entry in row n of Pascal's Triangle is odd, i.e. every binomial coefficient

$$\binom{n}{\ell} = \frac{n!}{\ell!\,(n-\ell)!}$$

is odd, $\ell = 0, 1, \ldots, n$.

pf: First, note that

$$n = 2^k - 1 = 2^k - 2 + 1$$
$$= 2(2^{k-1} - 1) + 1$$

is odd, so there are $(\ell = 0, 1, \ldots, n)$ $n+1$ coefficients $\binom{n}{\ell}$ to consider, an even number of coefficients. We know, moreover, that

$$\binom{n}{n} = \binom{n}{0} = 1$$

and, for the record, $\binom{n}{n-1} = \binom{n}{1} = n$ } all odd.

so it remains to check $\binom{n}{\ell}$ for $\ell = 2, \ldots, n-2$.

Suppose, therefore, that

$$2 \leq \ell \leq n-2$$

Now,

$$n! = (2^k - 1)!$$

$$= (2^k-1)(2^k-2)(2^k-3)\cdots(2^k-\ell)\,(2^k-1-\ell)!$$

so

$$\binom{n}{\ell} = \frac{n!}{\ell!\,(n-\ell)!}$$

$$= \frac{(2^k-1)(2^k-2)\cdots(2^k-\ell)\cdot(2^k-1-\ell)!}{\ell!\,(n-\ell)!} \qquad (2^k-1-\ell)! = (n-\ell)!$$

$$= \frac{(2^k-1)(2^k-2)\cdots(2^k-\ell)}{\ell\cdot(\ell-1)\cdots 3\cdot 2\cdot 1}$$

An observation is now in order:

odd

$$z^k - 1 = z^k - 1^k \quad \leftarrow \quad a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + b^{k-1})$$

$$= (z-1)(z^{k-1} + z^{k-2} + \cdots + 1)$$

$(z-1)$: $= 1$

$(z^{k-1} + z^{k-2} + \cdots + 1)$: $= z(z^{k-2} + \cdots + z + 1) + 1$

$$= z^{k-1} + z^{k-2} + \cdots + z^2 + z + 1$$

even

$$z^k - z = z(z^{k-1} - 1)$$

$$= z((z-1)(z^{k-2} + z^{k-3} + \cdots + z + 1))$$

$$= z(z^{k-2} + z^{k-3} + \cdots + 1)$$

z | $(z^{k-2} + z^{k-3} + \cdots + 1)$: odd

odd

$$z^k - 3 = z^k - z - 1$$

$$= z(z^{k-2} + z^{k-3} + \cdots + z + 1) - 1$$

even

$$z^k - 4 = z^2(z^{k-2} - 1)$$

$$= z^2(z^{k-3} + z^{k-4} + \cdots + z + 1)$$

z^2 | $(z^{k-3} + z^{k-4} + \cdots + z + 1)$: odd

etc. Thus, $z^k - r$, when r is even, allows us to factor out of $z^k - r$ all powers of z in r!

Back to $\binom{n}{\ell}$: we said above that

$$\binom{n}{\ell} = \frac{(z^k-1)(z^k-2)(z^k-3)\cdots(z^k-\ell)}{1\cdot 2\cdot 3\cdots \ell}$$

factor out of the evens & cancel →

$$= \frac{(z^k-1)\cdot 2(z^{k-1}-1)(z^k-3)\cdot 2(z^{k-2}-1)\cdots}{1\cdot 2\cdot 3\cdot 4\cdots \ell}$$

$$= \frac{\text{odd}\cdot\text{odd}\cdots\text{odd}}{\text{odd}\cdot\text{odd}\cdots\text{odd}}$$

= an odd # (see below)

By our observation on the previous page, all powers of 2 factored out upstairs cancel exactly w/ all powers of 2 downstairs, so we are left only with odds. Products of odds are odd (Ch. 4 #4), so both numerator & denom. are odd.

Now, for the punch line: if $\binom{n}{\ell}$ were even, say $\binom{n}{\ell} = 2m$, then (odd #)$\cdot 2m$ = (odd #) Impossible!