Corollary: 1) $$2^n = \sum_{k=0}^{n} \binom{n}{k}$$

2) $$0 = \sum_{k=0}^{n} (-1)^k \binom{n}{k}$$

3) $$2^{n-1} = \sum_{\substack{k=0 \\ k \text{ odd}}}^{n} \binom{n}{k} = \sum_{\substack{k=0 \\ k \text{ even}}}^{n} \binom{n}{k}$$

proof: 1) By the binomial theorem,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

For 1) we choose

$$x = y = 1.$$

2) For 2), choose

$$x = -1$$

$$y = 1.$$

3) From 2),

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

$$0 = \sum_{\substack{k=0 \\ k \text{ odd}}}^{n} \binom{n}{k} \underbrace{(-1)^k}_{=-1} + \sum_{\substack{k=0 \\ k \text{ even}}}^{n} \binom{n}{k} \underbrace{(-1)^k}_{=1}$$

$$0 = -\sum_{\substack{k=0 \\ k \text{ odd}}}^{n} \binom{n}{k} + \sum_{\substack{k=0 \\ k \text{ even}}}^{n} \binom{n}{k}$$

$$\Rightarrow \sum_{\substack{k=0 \\ k \text{ odd}}}^{n} \binom{n}{k} = \sum_{\substack{k=0 \\ k \text{ even}}}^{n} \binom{n}{k}$$

We know from 1) that

$$2^n = \sum_{k=0}^{n} \binom{n}{k} = 2 \sum_{\substack{k=0 \\ k \text{ even}}}^{n} \binom{n}{k},$$

so $$2^{n-1} = \sum_{\substack{k=0 \\ k \text{ even}}}^{n} \binom{n}{k} = \sum_{\substack{k=0 \\ k \text{ odd}}}^{n} \binom{n}{k}.$$

Lemma: Let $p \in \mathbb{N}$ be prime. Then

1) If $0 < k < p$, $k \in \mathbb{N}$,

then $p \mid \binom{p}{k}$.

2) $\forall\ m, n \in \mathbb{Z}$,

$$(m+n)^p \equiv m^p + n^p \mod p$$

proof: 1) $\binom{p}{k} = \dfrac{p!}{(p-k)!\,k!}$, so

$$p! = \binom{p}{k} \cdot (p-k)! \cdot k!$$

$p \mid (p!)$, so we

must have either

$p \mid \binom{p}{k}$, $p \mid (p-k)!$, or

$p \mid k!$. But since

$0 < k < p$, also $0 < p-k < p$

and so p is not one of the

terms in either $k!$ or $(p-k)!$.

Therefore, $p \nmid k!$ and $p \nmid (p-k)!$,

so we must have $p \mid \binom{p}{k}$.

2) By the binomial theorem,

$$(m+n)^p = \sum_{k=0}^{p} \binom{p}{k} m^k n^{p-k}.$$

But if $0 < k < p$, we showed

$p \mid \binom{p}{k}$, so

$$(m+n)^p \bmod p = \left(\sum_{k=0}^{p} \binom{p}{k} m^k n^{p-k} \right) \bmod p$$

$$\equiv \sum_{k=0}^{p} \left(\binom{p}{k} m^k n^{p-k} \bmod p \right)$$

$$\equiv \sum_{k=0}^{p} \binom{p}{k} \bmod p \cdot \left(m^k n^{p-k}\right) \bmod p$$

$\binom{p}{k} \equiv 0 \bmod p$ since $p \mid \binom{p}{k}$

$$\equiv \binom{p}{p} m^p \bmod p + \binom{p}{0} n^p \bmod p$$

$\binom{p}{p} = 1$, $\binom{p}{0} = 1$

$$\equiv m^p \bmod p + n^p \bmod p$$

$$\equiv (m^p + n^p) \bmod p$$

□

Theorem: (Fermat, little) Let $p \in \mathbb{N}$, p prime. Then

1) $\forall\, n \in \mathbb{Z}$,

$$n^p \equiv n \bmod p$$

2) if $p \nmid n$, $n \in \mathbb{Z}$,

then

$$n^{p-1} \equiv 1 \bmod p$$

proof: We'll establish this as a corollary of a larger theorem.

Fermat's Last Theorem

Start: $x^2+y^2=z^2$. Are there solutions in $\mathbb{N}$ to this equation? Namely, are there $x,y,z \in \mathbb{N}$ that satisfy this equation?

Yes! $x=3$, $y=4$, $z=5$ will work. In fact, there are infinitely many solutions in $\mathbb{N}$ to this equation, called Pythagorean Triples.

What about solutions in $\mathbb{N}$ to

$$x^3+y^3=z^3 \; ? \quad \text{or}$$

$$x^{101}+y^{101}=z^{101} \; ?$$

There are no solutions in $\mathbb{N}$!

Mainly due to Andrew Wiles in the 1990's - roughly 300 pages of hard math!

The only solutions in $\mathbb{N}$ to

$x^k+y^k=z^k$ occur when $k=1$ or $k=2$! $(k\in\mathbb{N})$

Euler's φ Function

This is called the "totient" function.

Let $n \in \mathbb{N}$. We define $\varphi(n)$ to be the cardinality of all $k \in \mathbb{N}$, $k < n$, with $\gcd(k, n) = 1$.

$\varphi(2) = 1$

$\varphi(3) = 2$

$\varphi(4) = 2 \neq \varphi(2)^2$

$\varphi(5) = 4$

$\varphi(6) = 2 = \varphi(2) \cdot \varphi(3)$

$\varphi(7) = 6$

$\varphi(8) = 4$

$\varphi(9) = 6$

$\vdots$

Proposition: ($\varphi(n)$ and multiplicativity)

If $\gcd(n,m)=1$, then

$$\varphi(nm)=\varphi(n)\varphi(m).$$

proof: Let

$$A=\{k\in\mathbb{N} \mid 1\le k<n,\ \gcd(k,n)=1\}$$

$$B=\{\ell\in\mathbb{N} \mid 1\le \ell<m,\ \gcd(\ell,m)=1\}$$

$$C=\{s\in\mathbb{N} \mid 1\le s<nm,\ \gcd(s,nm)=1\}$$

By the Chinese Remainder Theorem,

if $k \in A$ and $\ell \in B$, since

$\gcd(m,n) = 1$, $\exists\ s \in C$,

$$s \equiv k \mod n$$

$$s \equiv \ell \mod m .$$

Moreover, s is unique up to

congruence modulo mn.

This fact implies that there

is a well-defined function

$$f : A \times B \to C$$ such that

$$f((k,\ell)) = s$$

where $s \equiv k \bmod n$, $s \equiv \ell \bmod m$.

$$|A \times B| = |A| \cdot |B| = \varphi(n)\varphi(m)$$

$$|C| = \varphi(nm).$$

We will show that f is a bijection, so that

$$\varphi(n)\varphi(m) = |A \times B| = |f(A \times B)| = |C| = \varphi(nm).$$

injectivity

Suppose $(k,\ell), (a,b) \in A \times B$,

$f((k,\ell)) = f((a,b)) = S$.

Then by definition of S,

$S \equiv k \bmod n \equiv a \bmod n$,

so $n \mid (k-a)$. But

$|\leq k, a < n$, so $k-a=0$

and $a=k$. Similarly, since

$S \equiv \ell \bmod m = b \bmod m$,

we get $\ell = b$. Therefore,

f is injective.

Surjectivity: Let $s \in C$. Let

$k \equiv s \bmod n$, $1 \leq k < n$

$\ell \equiv s \bmod m$, $1 \leq \ell < m$.

Since $\gcd(s, mn) = 1$,

then $\gcd(k, n) = 1$ and

$\gcd(\ell, n) = 1$ $\Rightarrow$

$(k, \ell) \in A \times B$, so that

$f((k, \ell)) = s$. Therefore,

f is surjective.

We know f is a bijection,

so

$$\varphi(n)\varphi(m) = |A \times B| = |f(A \times B)| = |C| = \varphi(nm).$$