$\gcd(m,n) = m \cdot lc_1(m,n) + n \cdot lc_2(m,n)$

Multiplicative inverses in modular arithmetic

Corollary 92 *For all positive integers* m *and* n,

1. $n \cdot \mathrm{lc}_2(m,n) \equiv \gcd(m,n) \pmod{m}$, *and*
2. *whenever* $\gcd(m,n) = 1$,

   $\left[\mathrm{lc}_2(m,n)\right]_m$ *is the multiplicative inverse of* $[n]_m$ *in* $\mathbb{Z}_m$.

$n \cdot lc_2(m,n) \equiv 1 \pmod{m}$ if $\gcd(m,n) = 1$

$[n]_m \cdot [lc_2(m,n)]_m$

Key exchange

Mathematical modelling:

- Encrypt and decrypt by means of modular exponentiation:

$$[k^e]_p \qquad\qquad [\ell^d]_p$$

- Encrypting-decrypting have no effect:

By Fermat's Little Theorem,

$$k^{1+c\cdot(p-1)} \equiv k \pmod{p}$$

for every natural number c, integer k, and prime p.

- Consider d, e, p such that $e \cdot d = 1 + c \cdot (p-1)$; equivalently,

$$d \cdot e \equiv 1 \pmod{p-1} \ .$$

$(k^e)^d \equiv k \pmod{p}$

Lemma 93 *Let* p *be a prime and* e *a positive integer with* $\gcd(p-1, e) = 1$*. Define*

$$d = \left[\mathrm{lc}_2(p-1, e) \right]_{p-1} \ .$$

Then, for all integers k*,*

$$(k^e)^d \equiv k \pmod{p} \ .$$

PROOF:

Natural Numbers and mathematical induction

We have mentioned in passing that the natural numbers are generated from zero by succesive increments. This is in fact the defining property of the set of natural numbers, and endows it with a very important and powerful reasoning principle, that of *Mathematical Induction*, for establishing universal properties of natural numbers.

Principle of Induction

Let $P(m)$ be a statement for m ranging over the set of natural numbers $\mathbb{N}$.

If

BASE CASE:

- the statement $P(0)$ holds, and

INDUCTIVE STEP:

- the statement

$$\forall n \in \mathbb{N}.\ \big(\ P(n) \implies P(n+1)\ \big)$$

also holds

then

- the statement

$$\forall m \in \mathbb{N}.\, P(m)$$

holds.

Binomial Theorem

Theorem 29 *For all* $n \in \mathbb{N}$,

$$P(n) \equiv \left[(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k \right].$$

PROOF:

BASE CASE: Show $P(0)$; That is,

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

$$1 = \binom{n}{0} x^0 y^0 = 1 \quad \checkmark$$

INDUCTIVE STEP: $\forall n \in \mathbb{N}.\ P(n) \Rightarrow P(n+1)$

Let $n \in \mathbb{N}$.

Assume: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$ (IH) — Induction hypothesis

RTP: $(x+y)^{n+1} \stackrel{?}{=} \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k$

$\| $

$(x+y) \cdot (x+y)^n$

$\|$ by (IH)

$(x+y) \cdot \left[\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \right]$

$\|$

$x^{n+1} + \boxed{\sum_{k=1}^{n} \binom{n+1}{k} x^{n+1-k} y^k} + y^{n+1}$

$$(x+y)\left[\sum_{k=0}^{n}\binom{n}{k}\, x^{n-k}\, y^{k}\right]$$

$$= x\cdot\sum_{k=0}^{n}\binom{n}{k}\, x^{n-k}\, y^{k} + y\cdot\sum_{k=0}^{n}\binom{n}{k}\, x^{n-k}\, y^{k}$$

$$= \sum_{k=0}^{n}\binom{n}{k}\, x^{n-k+1}\, y^{k} + \sum_{k=0}^{n}\binom{n}{k}\, x^{n-k}\, y^{k+1}$$

$$= x^{n+1} + \boxed{\sum_{k=1}^{n}\binom{n}{k}\, x^{n-k+1}\, y^{k} + \sum_{k=0}^{n-1}\binom{n}{k}\, x^{n-k}\, y^{k+1}} + y^{n+1}$$

$$\sum_{k=1}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n-1} \binom{n}{k} x^{n-k} y^{k+1}$$

$$= \sum_{k=1}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=1}^{n} \binom{n}{k-1} x^{n-k+1} y^k$$

$$= \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] \cdot x^{n-k+1} \cdot y^k$$

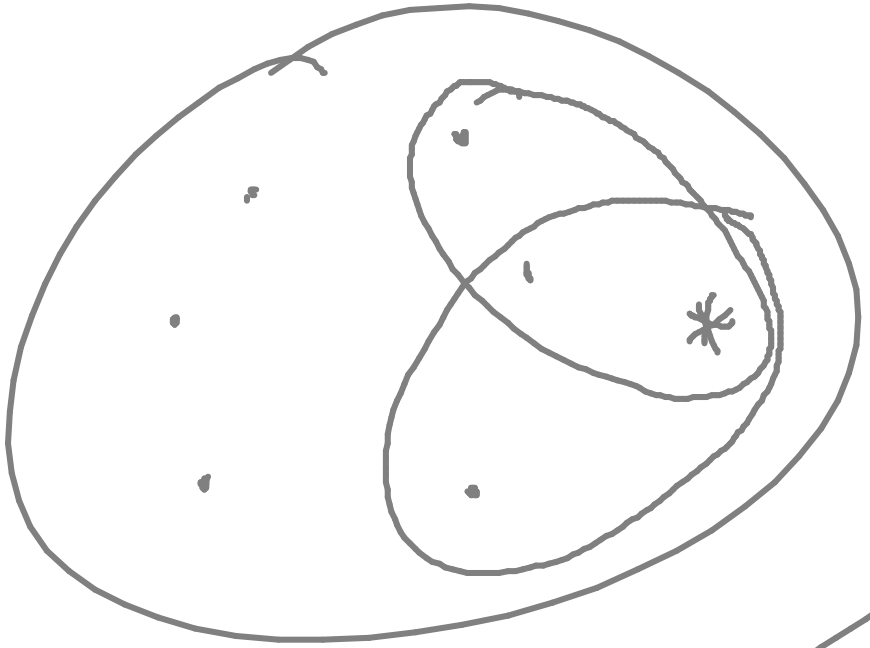
$$\overset{?}{=} \sum_{k=1}^{n} \binom{n+1}{k} x^{n+1-k} y^k$$

if Lemma:

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

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

To count $\binom{n+1}{k}$ is to count all the subsets of size k with a * plus all the subsets of size k without the *



$\binom{n}{k}$

$\binom{n}{k-1}$

Principle of Induction

from basis ℓ

Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ.

If

- $P(\ell)$ holds, and
- $\forall\, n \geq \ell$ in $\mathbb{N}$. $\big(\, P(n) \implies P(n+1) \,\big)$ also holds

then

- $\forall\, m \geq \ell$ in $\mathbb{N}$. $P(m)$ holds.

Let n be a nat. number $\geq \ell$ arbitrary.

Assume: $P(\ell) \wedge P(\ell+1) \wedge \ldots \wedge P(n)$ RTP: $P(n+1)$

Principle of Strong Induction

from basis ℓ and Induction Hypothesis $P(m)$.

Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ.

If both

BASE CASE

- $P(\ell)$ and

INDUCTIVE STEP

- $\forall n \geq \ell \text{ in } \mathbb{N}. \left(\left(\forall k \in [\ell..n]. P(k) \right) \implies P(n+1) \right)$

hold, then

- $\forall m \geq \ell \text{ in } \mathbb{N}. P(m)$ holds.

Fundamental Theorem of Arithmetic

Proposition 95 *Every positive integer greater than or equal 2 is a prime or a product of primes.*

PROOF: $\forall n \geq 2 . P(n)$

$P(n) \equiv^{def}$ n is prime or n is a product of primes.

BASE CASE: Show $P(2)$; That is,

2 is prime or 2 is a product of primes.

Holds since 2 is prime.

INDUCTIVE STEP:

Let $n \geq 2$ be arbitrary.

Assume: $P(2) \wedge P(3) \wedge \cdots \wedge P(n)$ (SIH)

RTP: $P(n+1)$; that is,

$n+1$ is prime or $n+1$ is a product of primes

Case(1): $n+1$ is prime; we are done.

Case(2): $n+1$ is not prime; so $n+1 = a \cdot b$ for natural numbers a and b that are greater than or equal 2 and less than or equal n.

So we have, by (SIH), $P(a)$ and $P(b)$

So a and b are primes or products of primes. Therefore $n+1 = a \cdot b$ is a product of primes.

$\boxtimes$

Theorem 96 (Fundamental Theorem of Arithmetic) *For every positive integer* n *there is a unique finite ordered sequence of primes* $(p_1 \leq \cdots \leq p_\ell)$ *with* $\ell \in \mathbb{N}$ *such that*

$$n = \prod(p_1, \ldots, p_\ell) \ .$$

notation of product of $p_1, \ldots, p_\ell$

$\prod() \overset{\text{def}}{=} 1$

PROOF:

$n = \pi(p_1 \cdots p_\ell)$
$p_1 \leq \cdots \leq p_\ell$ primes

$n = \pi(q_1 \cdots q_k)$
$q_1 \leq \cdots \leq q_k$ primes.

$\overset{?}{\Longrightarrow}$ $\ell = k$ and $p_1 = q_1 \wedge \cdots \wedge p_\ell = q_k$.

① $p_1 \mid n = \pi(p_1 - p_e) = \pi(q_1 - q_k)$

$\Rightarrow p_1 \mid q_j \qquad q_1 \le p_1$

② $q_1 \mid n = \pi(q_1 - q_k) = \pi(p_1 - p_e)$

$q_1 \mid p_j \qquad p_1 \le q_1$

$\Rightarrow p_1 = q_1 \Rightarrow \pi(p_2, \cdots, p_e) = \pi(q_2, \cdots, q_k)$