PROPOSITION

For a positive integer m, the following are equivalent:

(1) $m = 1$.

(2) For all integers a and b, $a \equiv b \pmod{m}$.

(3) $1 \equiv 0 \pmod{m}$.

PROOF: (1) $\Rightarrow$ (2) Let a and b be int.

RTP: $a \equiv b \pmod{1}$, which is the case because $a - b$ is a multiple of 1.

(2) $\Rightarrow$ (3) By instantiation.

(3) $\Rightarrow$ (1) Assume $1 \equiv 0 \pmod{m}$

RTP : $m = 1$

By assumption, $1 = k.m$ for an int k.

So m is either 1 or -1 but since it is positive $m = 1$.

$\square$

A little more arithmetic

Corollary 33 (The Freshman's Dream) *For all natural numbers* m, n *and primes* p,

$$(m+n)^p \equiv m^p + n^p \pmod{p} .$$

PROOF: Let m and n be nat. and let p be a prime.

We have $(m+n)^p = \sum_{i=0}^{p} \binom{p}{i} m^i n^{p-i}$

$= n^p + \sum_{i=1}^{p-1} \binom{p}{i} m^i n^{p-i} + m^p$

Recall $\binom{p}{i} \equiv 0 \pmod{p}$

$1 \le i \le p-1$

Lemma

$$a_i \equiv b_i \pmod m$$

$$\Rightarrow$$

$$\sum_i a_i \equiv \sum_i b_i \pmod m$$

$$\prod_i a_i \equiv \prod_i b_i \pmod m$$

$$(m+n)^p = m^p + n^p + \sum_{i=1}^{p-1} \binom{p}{i} m^i n^{p-i}$$

$$\binom{p}{i} \equiv 0 \pmod p$$

$$\equiv 0 \pmod p$$

$\boxtimes$

Corollary 34 (The Dropout Lemma) *For all natural numbers* m *and primes* p*,*

$$(\mathrm{m}+1)^{\mathrm{p}} \equiv \mathrm{m}^{\mathrm{p}} + 1 \pmod{\mathrm{p}} \ .$$

Proposition 35 (The Many Dropout Lemma) *For all natural numbers* m *and* i*, and primes* p*,*

$$(\mathrm{m}+\mathrm{i})^{\mathrm{p}} \equiv \mathrm{m}^{\mathrm{p}} + \mathrm{i} \pmod{\mathrm{p}} \ .$$

PROOF: Let m and i be nat. and p a prime.

Consider

$$(m+i)^p = (m+\overbrace{1+1+\cdots+1}^{i \text{ times}})^p$$

$$\equiv (m+\underbrace{1+\cdots+1}_{i-1 \text{ times}})^p + 1$$

$$\equiv \Big(m + \underbrace{1 + \cdots + 1}_{i-2 \text{ times}}\Big)^p + \underbrace{1+1}_{2 \text{ times}}$$

$$\equiv \Big(m+1 + \underbrace{\cdots + 1}_{i-3 \text{ times}}\Big)^p + \underbrace{1+1+1}_{3 \text{ times}}$$

$$\vdots$$

$$\equiv \Big(m + \underbrace{1 + \cdots + 1}_{i-k \text{ times}}\Big)^p + \underbrace{1 + \cdots + 1}_{k \text{ times}}$$

$$\equiv m^p + \Big(\underbrace{1 + \cdots + 1}_{0 \text{ times}}\Big) = m^p + i. \qquad \text{for } k = i$$

$\boxtimes$

The Many Dropout Lemma (Proposition 35) gives the fist part of the following very important theorem as a corollary.

Theorem 36 (Fermat's Little Theorem) *For all natural numbers* i *and primes* p*,*

1. $\mathrm{i}^{\mathrm{p}} \equiv \mathrm{i} \pmod{\mathrm{p}}$*, and*
2. $\mathrm{i}^{\mathrm{p}-1} \equiv 1 \pmod{\mathrm{p}}$ *whenever* i *is not a multiple of* p*.*

$p \mid (i^p - i) = i(i^{p-1} - 1)$
⇓ by prime fact. Thm
$p \mid i^{p-1} - 1$

The fact that the first part of Fermat's Little Theorem implies the second one will be proved later on .

NB

$$i^{p-1} \equiv 1 \pmod{p}$$

$$\| $$

$$i \cdot (i^{p-2})$$

$\}$ modulo p

i (which is not a multiple of p)

has a reciprocal!

Btw

1. Fermat's Little Theorem has applications to:
   (a) primality testing[a],
   (b) the verification of floating-point algorithms, and
   (c) cryptographic security.

[a] For instance, to establish that a positive integer $\mathfrak{m}$ is not prime one may proceed to find an integer $\mathfrak{i}$ such that $\mathfrak{i}^{\mathfrak{m}} \not\equiv \mathfrak{i} \pmod{\mathfrak{m}}$.

Negation

Negations are statements of the form

$$\boxed{\text{not } P}$$

or, in other words,

$$\boxed{P \text{ is not the case}}$$

or

$$\boxed{P \text{ is absurd}}$$

or

$$\boxed{P \text{ leads to contradiction}}$$

or, in symbols,

$$\boxed{\neg P}$$

A first proof strategy for negated goals and assumptions:

If possible, reexpress the negation in an *equivalent* form and use instead this other statement.

Logical equivalences

$$
\begin{aligned}
\neg(P \Longrightarrow Q) &\iff P \wedge \neg Q \\
\neg(P \Longleftrightarrow Q) &\iff P \Longleftrightarrow \neg Q \\
\neg(\forall x.\, P(x)) &\iff \exists x.\, \neg P(x) \\
\neg(P \wedge Q) &\iff (\neg P) \vee (\neg Q) \\
\neg(\exists x.\, P(x)) &\iff \forall x.\, \neg P(x) \\
\neg(P \vee Q) &\iff (\neg P) \wedge (\neg Q) \\
\neg(\neg P) &\iff P \\
\neg P &\iff (P \Rightarrow \mathbf{false})
\end{aligned}
$$

Theorem 37 *For all statements* P *and* Q,

$$(P \implies Q) \implies (\neg Q \implies \neg P) \quad .$$

PROOF: Let P and Q be statements.

Assume ① $P \Rightarrow Q$

RTP $\neg Q \Rightarrow \neg P$

Assume ② $\neg Q \Leftrightarrow (Q \Rightarrow \text{false})$

RTP: $\neg P \Leftrightarrow (P \Rightarrow \text{false})$

Assume ③ P

RTP false.

From ① and ③, we have ④ Q. From ② and ④, we have false. ☒

Proof by contradiction

The strategy for proof by contradiction:

To prove a goal P by contradiction is to prove the equivalent statement $\neg P \implies \mathbf{false}$

Proof pattern:

In order to prove

$$P$$

1. Write: We use proof by contradiction. So, suppose P is false.
2. Deduce a logical contradiction.
3. Write: This is a contradiction. Therefore, P must be true.

Scratch work:

Before using the strategy

Assumptions	Goal
	P
$\vdots$	

After using the strategy

Assumptions	Goal
	contradiction
$\vdots$	
$\neg P$	

Theorem 39 *For all statements* P *and* Q,

$$(\neg Q \implies \neg P) \implies (P \implies Q) \ .$$

PROOF: Let P and Q be statements

Assume ① $\neg Q \Rightarrow \neg P$

Assume ② P

RTP Q

By contradiction, assume ③ $\neg Q$.

Then, from ① and ③, we have ④ $\neg P$.

From ② and ④, we have an absurdity.

Hence, Q holds.

Lemma 41 *A positive real number* x *is rational iff*

$$\exists \textit{ positive integers } m, n : \quad x = m/n \wedge \neg(\exists \textit{ prime } p : \; p \mid m \wedge p \mid n) \qquad (\dagger)$$

PROOF: ($\Leftarrow$) Easy.

($\Rightarrow$) RTP: $x = a/b$ for int. a and b

$\Rightarrow$ ($\dagger$)

Assume: $x = a/b$ for pos. int a and b.

RTP: ($\dagger$)

We proceed by proof by contradiction.

To that end assume (†) is not the case, that is.

for all pos. int. m, n.

$$\neg(x = m/n) \vee (\exists \text{ prime } p.\ p \mid m \wedge p \mid n)$$

$\Leftrightarrow$

$$\left[\forall \text{ pos. int. } m.n \quad x = m/n \Rightarrow (\exists \text{ prime } p.\ p \mid m \wedge p \mid n)\right] (\dagger)$$

Recall $x = a/b$

By substitution

$$x = a/b \Rightarrow (\exists \text{ prime } p.\ p \mid a \wedge p \mid b)$$

Hence $\exists$ prime $p.\ p \mid a \wedge p \mid b$

So $a = p_0 \cdot a_1$ and $b = p_0 \cdot b_1$ for a prime p_0 and int. a_1, b_1

Then $x = a_1 / b_1$

By induction

$$x = a_1/b_1 \Rightarrow (\exists\, p \text{ prime} \cdot p \mid a_1 \wedge p \mid b_1)$$

Hence again.

$a_1 = p_1 \cdot a_2$ and $b_1 = p_1 \cdot b_2$ for a prime p_1 and int a_2, b_2

$(a = p_0 a_1 = p_0 \cdot p_1 \cdot a_2)$

"Iterating This argument" we have

$a = p_0 \cdot p_1 \cdot p_2 \cdots p_k \cdot a_{k+1}$ for primes $p_0 \ldots p_k$ and int a_{k+1}

It follows that

$a \geq 2^k$ for all k

This is absurd, and we are done. ⊠