A little arithmetic

Lemma 27  For all positive integers $p$ and natural numbers $m$, if $m = 0$ or $m = p$ then \( \binom{p}{m} \equiv 1 \pmod{p} \).

**Proof:** Let $p$ be a pos. int. and $m$ a nat. numer.

Assume $m = 0$ or $m = p$.

RTP: \( \binom{p}{m} \equiv 1 \pmod{p} \)

Consider $m = 0$. Then \( \binom{p}{0} = 1 \) and we are done.

Consider $m = p$. Then \( \binom{p}{p} = 1 \) and we are done.
Lemma 28  For all integers $p$ and $m$, if $p$ is prime and $0 < m < p$ then $(\binom{p}{m}) \equiv 0 \pmod{p}$.

Proof: Let $p$ and $m$ be integers.
Assume $p$ prime and $0 < m < p$.

Recall: $\binom{p}{m} = \frac{p!}{m!(p-m)!}$

Then
$$m!(p-m)!(\binom{p}{m}) = p(p-1)!$$

is a natural number

So $p$ divides $m!(p-m)!(\binom{p}{m})$. And $p$ does not divide $m!(p-m)!$. Therefore it divides $\binom{p}{m}$. 

$\Box$
The argument hinges on the prime factorization theorem and
\[ p | (a \cdot b) \Rightarrow (p | a \text{ or } p | b) \quad p \text{ prime} \]
So that
\[ (p | (a \cdot b) \text{ and } p | a) \Rightarrow p | b. \]
Proposition 29  For all prime numbers $p$ and integers $0 \leq m \leq p$, either $\binom{p}{m} \equiv 0 \pmod{p}$ or $\binom{p}{m} \equiv 1 \pmod{p}$.

PROOF: Let $p$ be a prime and $m$ an integer $0 \leq m \leq p$.

Case $m = 0$ or $m = p$: Then $\binom{p}{m} \equiv 1 \pmod{p}$.

Case $0 < m < p$: Then $\binom{p}{m} \equiv 0 \pmod{p}$.

Therefore either $\binom{p}{m} \equiv 0$ or $\binom{p}{m} \equiv 1 \pmod{p}$.

\[\Box\]
Newton's Binomial Formula

\[(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\]

Say \( n \) is a prime, what's

\[(x+y)^n \equiv \binom{n}{0} y^n + \binom{n}{1} x^n \pmod{n} \]

\[\equiv y^n + x^n.\]
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 natural numbers, and $p$ be a prime. Then

$$(m+n)^p = \sum_{i=0}^{p} \binom{p}{i} m^i n^{p-i} = m^p + n^p + \sum_{i=1}^{p-1} \binom{p}{i} m^i n^{p-i}.$$ 

Since $\binom{p}{i} \equiv 0 \pmod{p}$ for $0 < i < p$. Then, we are done. \(\blacksquare\)
NB: $a \equiv b \pmod{m} \quad x \equiv y \pmod{m}$

$\Rightarrow$

$a + x \equiv b + y \pmod{m}$

$a \cdot x \equiv b \cdot y \pmod{m}$
Corollary 34 (The Dropout Lemma)  For all natural numbers $m$ and primes $p$,

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

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

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

**Proof:** Let $m$ and $i$ be natural numbers, and $p$ be a prime. Consider

$$(m+i)^p = (m+\underbrace{1+1+\ldots+1}_{i \text{ times}})^p \equiv (m+\underbrace{1+\ldots+1}_{i-1 \text{ times}})^p + 1 = (m+\underbrace{1+1+\ldots+1}_{i-2 \text{ times}})^p + \underbrace{1+1}_{2 \text{ times}} = \ldots = (m+\underbrace{1+\ldots+1}_{i-k \text{ times}})^p + \underbrace{1+\ldots+1}_{k \text{ times}}$$
For $k = i$, we have

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

For $m = 0$,

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

Then

$$(i^p - i) \equiv 0 \pmod{p}$$

and so

$p$ divides $i(i^{p-1} - 1)$

From which we have $p$ divides $i(i^{p-1} - 1)$ whenever $p$ does not divide $i$. 
Thus, \[ i^{p-1} \equiv 1 \pmod{p} \]
whenever \( p \) does not divide \( i \).

Then \[ i \cdot (i^{p-2}) \equiv 1 \pmod{p} \]
whenever \( i \neq 0 \pmod{p} \).

So modulo \( p \), \( i^{p-2} \) is a reciprocal of \( i \) for \( i \neq 0 \pmod{p} \).
Fermat’s Little Theorem

The Many Dropout Lemma (Proposition 35) gives the first 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. $i^p \equiv i \pmod{p}$, and
2. $i^{p-1} \equiv 1 \pmod{p}$ whenever $i$ is not a multiple of $p$.

The fact that the first part of Fermat’s Little Theorem implies the second one will be proved later on.
Every natural number $i$ not a multiple of a prime number $p$ has a reciprocal modulo $p$, namely $i^{p-2}$, as $i \cdot (i^{p-2}) \equiv 1 \pmod{p}$. 
Btw

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

\[ i^m \equiv i \pmod{m} \]

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

Negations are statements of the form

\[ \neg P \]

or, in other words,

\[ P \text{ is not the case} \]

or

\[ P \text{ is absurd} \]

or

\[ P \text{ leads to contradiction} \]

or, in symbols,

\[ \neg P \]
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**

\[
\begin{align*}
\neg( P \implies Q ) & \iff P \land \neg Q \\
\neg( P \iff Q ) & \iff P \iff \neg Q \\
\neg(\forall x. P(x)) & \iff \exists x. \neg P(x) \\
\neg( P \land Q ) & \iff (\neg P) \lor (\neg Q) \\
\neg(\exists x. P(x)) & \iff \forall x. \neg P(x) \\
\neg( P \lor Q ) & \iff (\neg P) \land (\neg Q) \\
\neg(\neg P) & \iff P \\
\neg P & \iff (P \implies \text{false})
\end{align*}
\]
Theorem 37  For all statements $P$ and $Q$, 

$$(P \Rightarrow Q) \iff (\neg Q \Rightarrow \neg P)$$.

PROOF: Let $P$ and $Q$ be statements.

Assume $P \Rightarrow Q$. 

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

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

Assume $P$

RTP: false

By 1 & 2, we have $Q$. By 3 & 4, we have false.

— 133 —
Proof by contradiction

Amongst the equivalences for negation, we have postulated the somewhat controversial:

\[ \neg \neg P \iff P \]

which is classically accepted.

In this light,

to prove \( P \)

one may equivalently

prove \( \neg P \implies \text{false} \);

that is,

assuming \( \neg P \) leads to contradiction.

This technique is known as proof by contradiction.
The strategy for proof by contradiction:

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

**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
\[ P \]
\[ \vdots \]
\[ \vdots \]

After using the strategy

Assumptions  Goal
contradiction
\[ \neg P \]
Theorem 39  For all statements $P$ and $Q$,

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

PROOF: Let $P$ and $Q$ be statements.

1. Assume $\neg Q \Rightarrow \neg P$
2. Assume $P$
3. Assume $\neg Q$
4. RTP: False

By (1) & (2), we have $\neg P$. And (2) & (4) is a contradiction. \(\Box\)
Proof by contrapositive

Corollary 40  For all statements $P$ and $Q$,

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

Btw  Using the above equivalence to prove an implication is known as \textit{proof by contrapositive}.

Corollary 41  For every positive irrational number $x$, the real number $\sqrt{x}$ is irrational.