P8: product of odd integers

Goal: $\forall m, n \in \mathbb{Z} : (m, n \text{ odd} \implies m \cdot n \text{ odd})$

Assume:
1. $m, n \in \mathbb{Z}$
2. m, n odd

$$\begin{aligned} m &= 2a + 1 \\ n &= 2b + 1 \\ m \cdot n &= 2(2ab + a + b) + 1 \end{aligned}$$

P10: rational square root

Goal: $\forall x \in \mathbb{R}^+ : \sqrt{x} \text{ rational} \implies x \text{ rational}$

Assume:
1. $x \in \mathbb{R}^+$
2. $\sqrt{x}$ rational

$$\begin{aligned} \sqrt{x} &= \frac{p}{q} \\ x &= \frac{p^2}{q^2} \end{aligned}$$

T11: transitivity of implication

Goal: $\forall P_1, P_2, P_3 : ((P_1 \implies P_2) \land (P_2 \implies P_3) \implies (P_1 \implies P_3))$

Assume:
1. $P_1 \implies P_2$
2. $P_2 \implies P_3$
3. P_1

$$\begin{aligned} &\implies P_2 \text{ by } (1) \\ &\implies P_3 \text{ by } (2) \end{aligned}$$

P18: lineararity of congruence

Goal: $\forall m, n \in \mathbb{Z}^+ \land a, b \in \mathbb{Z} : a \equiv b \pmod{m} \iff n \cdot a \equiv n \cdot b \pmod{n \cdot m}$

Assume:
1. $m, n \in \mathbb{Z}^+$
2. $a, b \in \mathbb{Z}$

$$\begin{aligned} a \equiv b \pmod{m} &\iff a - b = k \cdot m \\ &\iff n \cdot a - n \cdot b = k \cdot n \cdot m \\ &\iff n \cdot a \equiv n \cdot b \pmod{n \cdot m} \end{aligned}$$

T19

Goal: $\forall n \in \mathbb{Z} : (6|n \iff 2|n \land 3|n)$

Assume:
1. $n \in \mathbb{Z}$

$$
\begin{aligned}
6|n &\implies n = 6k \\
&\implies n = 3 \cdot (2k) \wedge n = 2 \cdot (3k) \\
&\implies 3|n \wedge 2|n
\end{aligned}
$$

$$
\begin{aligned}
n &= 2a \\
n &= 3b \\
3n &= 6a \\
2n &= 6b \\
n &= 6(a-b) \\
&\implies 6|n
\end{aligned}
$$

P21

Goal: $\forall k \in \mathbb{Z}^+ : \exists i, j \in \mathbb{Z} \wedge 4k = i^2 - j^2$

Assume:
1. $k \in \mathbb{Z} +$

Let $i = k + 1$ and $j = k - 1$, then $i^2 - j^2 = 4k$

T23: transitivity of divisiblity

Goal: $\forall l, m, n \in \mathbb{Z} : (l|m \wedge m|n \implies l|n)$

Assume:
1. $l, m, k \in \mathbb{Z}$
2. $l|m \wedge m|n$

$$
\begin{aligned}
m &= a \cdot l \\
n &= b \cdot m \\
n &= (a \cdot b) \cdot l \\
&\implies 1|n
\end{aligned}
$$

T24: uniqueness of congruence

Goal: $\forall m \in \mathbb{Z}^+ \wedge n \in \mathbb{Z} : \exists! z \wedge 0 \leq z < m \wedge z \equiv n \pmod m$

Assume:
1. $m \in \mathbb{Z}^+ \wedge n \in \mathbb{Z}$

Missing
Goal: $\exists z \wedge 0 \leq z < m \wedge z \equiv n \pmod m$

Assume:
1. $0 \leq z < m \wedge z \equiv n \pmod m$
2. $0 \leq z' < m \wedge z' \equiv n \pmod m$

$$
\begin{aligned}
& z \equiv z' \pmod m \\
\implies & z - z' = k \cdot m \\
& -m < z - z' < m \\
\implies & k = 0 \\
\implies & z = z'
\end{aligned}
$$

P25: square modulo 4

Goal: $\forall n \in \mathbb{Z} : n^2 \equiv 0 \pmod 4 \vee n^2 \equiv 1 \pmod 4$

Case $n = 2k$

$n^2 \equiv 4k^2 \equiv 0 \pmod 4$

Case $n = 2k + 1$

$n^2 \equiv 4k^2 + 4k + 1 \equiv 1 \pmod 4$

L27: ends of combinations

Goal: $\forall p \in \mathbb{Z}^+ \wedge m \in \mathbb{N} : \left(m = 0 \vee m = p \implies \binom{p}{m} \equiv 1 \pmod{p}\right)$

Assume:
1. $p \in \mathbb{Z}^+ \wedge m \in \mathbb{N}$

Case: $m = 0$

$$\binom{p}{0} \equiv 1 \pmod{p}$$

Case: $m = p$

$$\binom{p}{0} \equiv 1 \pmod{p}$$

L28: non-ends of combinations

Goal: $\forall p \text{ prime} \wedge m \in \mathbb{Z} : \left(0 < m < p \implies \binom{p}{m} \equiv 0 \pmod{p}\right)$

Assume:
1. $p \text{ prime} \wedge m \in \mathbb{Z}$
2. $0 < m < p$

$$\begin{aligned}\binom{p}{m} &\equiv \frac{p!}{(p-m)!m!} \\ &\equiv p \cdot \frac{(p-1)!}{(p-m)!m!} \\ &\equiv 0 \pmod{p}\end{aligned}$$

As p is only cancelled if a prime factor of p is in $(p-m)!m!$, the only prime factors of p are 1 and p, all prime factors of $(p-m)!m!$ are less than p.

P29: ends and non-ends of combinations

Goal: $\forall p \text{ prime} \wedge m \in \mathbb{Z} \wedge 0 \leq m \leq p : \binom{p}{m} \equiv 0 \pmod{p} \vee \binom{p}{m} \equiv 1 \pmod{p}$

Assume:
1. $p \text{ prime} \wedge m \in \mathbb{Z}$
2. $0 \leq m \leq p$

Case: $m = 0 \vee m = p$

$$\binom{p}{m} \equiv 1 \pmod{p}$$

Case $0 < m < p$

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

C33: the freshman's dream

Goal: $\forall m, n \in \mathbb{N} \wedge p \text{ prime} : (m+n)^p \equiv m^p + n^p \pmod{p}$

Assume:
1. $m, n \in \mathbb{N} \wedge p \text{ prime}$

$$\begin{aligned}(m+n)^p &\equiv \sum_{k=1}^{p} \binom{p}{k} m^{p-k} n^k \\ &\equiv m^p + n^p \pmod{p}\end{aligned}$$

C34: the dropout lemma

Goal: $\forall m \in \mathbb{N} \wedge p \text{ prime} : (m+1)^p \equiv m^p + 1 \pmod{p}$

Special case of (C33), $n = 1$

C35: the many dropout lemma

Goal: $\forall m, i \in \mathbb{N} \wedge p \text{ prime} : (m+i)^p \equiv m^p + 1 \pmod{p}$

Assume:
1. $m, i \in \mathbb{N}$
2. p prime

$$\begin{aligned}(m+i)^p &\equiv (m+i-1)^p + 1 \\ &\equiv (m+i-2)^p + 1 + 1 \\ &\vdots \\ &\equiv m^p + i \pmod{p}\end{aligned}$$

T36: Fermat's little theorem

Goal: $\forall i \in \mathbb{N} \wedge p \text{ prime} : i^p \equiv i \pmod{p}$

Special case of (C35), $m = 0$