Zac Foteff
CPSC 353

Project 3

(1) Extended Euclid: Let a, b be integers with a or b non-zero, that implies that there exist integers s, t such that $as + bt = \gcd(a, b)$

(2) $34720 = 2^5 \cdot 5 \cdot 7 \cdot 31$

(3) Let n be a positive integer. Two integers a, b are said to be congruent mod n ($a \equiv b \mod n$) if $a - b = kn$ for some int k

(4) $n = 1! + 2! + \dots + 100!$. The remainder must be $0 \leq r < 12$.
Every element greater than $4!$ is a multiple of 12, making the remainder 0 mod 12. Since all elements greater than $4!$ are congruent, that means the remainder would be $1! + 2! + 3!$

5 **Claim.** If $a \mid bc$ with a, b relatively prime, then $a \mid c$.

Proof.

Since we know a, b are relatively prime $\Rightarrow aS + bT = 1$

by extended Euclid.

Let c be an integer

$$acS + bcT = c$$

$a \mid acS$ & $a \mid bcT$, following that $a \mid bc$

$\therefore a \mid c$

(6) **Claim:** Any two integers are congruent mod 1

Proof:

Let x, y be integers

According to the congruence & division algorithm,

$x \equiv y \mod 1$ if and only if x and y yield the same remainder when divided by 1

Suppose $1 | x \Rightarrow$ $x = 1q + r$ for some ints q, r

$x = 1(x) + (0)$

Suppose $1 | y \Rightarrow$ $y = 1q + r$ for some ints q, r

$y = 1(y) + (0)$

Since both $1|x$ & $1|y$ both yield remainders of 0,

x, y are congruent mod 1

$\therefore$ Any two integers are congruent mod 1

(7) **Claim:** Any two integers are congruent mod 2 if both are even, or both are odd

Proof:

Let x, y be odd integers of the form $2k+1$

Suppose $2 | x$, according to the congruence and division algorithm

$x = 2q + r \Rightarrow r = x - 2q \Rightarrow r = (2k+1) - 2q$

Suppose $2 | y$, according to the congruence and division algorithm

$y = 2q + r \Rightarrow r = y - 2q \Rightarrow r = (2k+1) - 2q$

Since $x, y \mod 2$ both yield remainders of $r = (2k+1) - 2q$,

any 2 integers are congruent mod 2 if both are odd

Let x, y be even integers of the form $2k$

Suppose $2|x$, according to the congruence and division algorithm

$x = 2q + r \Rightarrow r = x - 2q \Rightarrow r = 2k - 2q$

Suppose $2|y$, according to the congruence and division algorithm

$y = 2q + r \Rightarrow r = y - 2q \Rightarrow r = 2k - 2q$

Since $x, y \bmod 2$ both yield remainders of $r = 2k + 2q$,

any 2 integers are congruent mod 2 if both are even

$\therefore$ Any 2 integers are congruent mod 2 if both are even, or both are odd

(8) Claim: If $x \equiv y \bmod n$, then $x \equiv (y + pn) \bmod n$ (Modulus Addition)

Let x, y, p, n be integers with $n > 0$.

$x \equiv (y + p_n) \bmod n$ can be expressed $n | (y + p_n)$

By the distributive property $n | (y + p_n) = n|y + n|p_n$

$n | p_n \Rightarrow p_n = nq + r \Rightarrow p_n = p_n + r$

So $n | p_n = 0$, which means that $n | (y + p_n) = n|y$

$\therefore$ If $x \equiv y \bmod n$ $(n|y)$, then $x \equiv (y + p_n) \bmod n$ $(n|y)$

(9) Claim: If $a \equiv b \bmod n$, $a^k \equiv b^k \bmod n$ for all integers k

Let a, b, n be integers where $n > 0$

Since a is congruent to b mod n, that means $a - b = cn$ for some int c according to the definition of congruence

$a - b = cn \Rightarrow a = b + cn$

$a^k = (b + cn)^k = b^k + kb^{(k-1)}cn + \ldots$ by the binomial theorum

$a^k - b^k = kb^{(k-1)}cn + \ldots$

Since every successive element is a multiple of n

$a^k \equiv b^k \bmod n$

10) 41 divides $2^{20}-1$ or $2^{20}-1 \bmod 41 = 0$

$2^{20}-1 \bmod 41 = 0 \Rightarrow 2^{20}-1-0 = 41c$

$(2^{10}+1)(2^{10}-1) = 41c$

$(1025)(1023) = 41c$

$(25)(41)(1023) = 41c$

$(25)(1023) = c$

Since there exists a number c such that $2^{20}-1 = 41c$, 41 divides $2^{20}-1$