CPSC 353 Project 3 Katie Stevens

① Extended Euclid Theorem

Given integers a and b with at least one of a, b non-zero,
There exists integers S and T such that
$aS + bT = gcd(a, b)$

② 34720 in canonical form
$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 \cdot 31$

③ Congruence
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 integer, k

④ $n = 1! + 2! + 3! + \ldots + 100!$
$n \equiv b \mod 12$ Let b equal to some integer
There exists a factor of 12 in every term 4! to 100! in n.
Find the remainder for terms 1! to 3! divided by 12.
$(1) + (1 \cdot 2) + (3 \cdot 2 \cdot 1) = 9$
The remainder is 9
$\boxed{n \equiv 9 \mod 12}$

(5) If $a|bc$ with a and b relatively prime, then $a|c$

Using extended euclid and knowing a and b are relatively prime we get

$\gcd(a, b) = 1$ so, $as + bT = 1$

This gives us

$\frac{bT}{as} = 1$

Now, using $a|bc$ we get

$\frac{bTc}{as}$, c lets $\frac{bT}{as}$ work

therefore, $a|c$

(6) Any two integers are congruent mod 1.

Given integers a and b

$a - b = 1k$, for some integer k

Any integer divides into 1.

Therefore,

$a \equiv b \mod 1$

7. Any two integers are mod 2 if both are even or odd.
Must satisy $a-b=2k$ for any integer k

Even:

Let $a=2l$ and $b=2m$

$a-b=2k$

$2l-2m=2k$

$2(l-m)=2k$

Since any two integers can go into any integer k, any two even integers satisfy $a \equiv b \bmod 2$

Odd:

Let $a=2l+1$ and $b=2m+1$

$a-b=2k$

$(2l+1)-(2m+1)=2k$

$2l-2m=2k$

$2(l-m)=2k$

Since any two integers can go into any integer k any two odd integers satisfy $a \equiv b \bmod 2$

8. Let x, y, P, n be integers $n>0$
if $x \equiv y \pmod n$, then $x \equiv (y+pn) \pmod n$

$x-y=kn$ for some integer k, $k>0$

$x-y-pn=kn-pn$

$x-y-pn=n(k-p)$

$x-(y+pn)=n(k-p)$

$x \equiv y+pn \bmod n$

(9) For any positive integer k

If $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$

$a - b = jn$ for any integer j

$(a-b)^k = (jn)^k$

$a^k - b^k = j^k n$, j^k scales with $a^k - b^k$ therefore,

$a^k \equiv b^k \pmod{n}$

(10) Using $a^k \equiv b^k \pmod{n}$ show that 41 divides $2^{20} - 1$

$2^{20} \equiv 1 \bmod 41$

$2^{20} = (2^5)^4 = (32)^4 \rightarrow 32 \equiv -9 \bmod 41$

$32^4 = (-9)^4 \bmod 41 \rightarrow (-9)^4 = 81^2$

$81 \equiv -1 \bmod 41$

$32^4 \equiv (-1)^4 \bmod 41$

therefore,

$2^{20} \equiv 1 \bmod 41$