Assignment: Project 2
Name 1: Jonathan Smoley
Name 2: Samuel Sovi
GitHub Name: JT2M0L3Y

1. State the theorem that we called Extended Euclid.

Let a, b be integers with at least one of a, b non-zero

Then ∃ integers s, t such that $as + bt = gcd(a)$

In particular, if a,b are relatively prime, $as + bt = 1$

2. We said in class that any positive integer > 1 can be written uniquely in canonical form. Write 34720 in canonical form.

Canonical form: factorization of a number into primes.

Factorization:
34720
$2 * 17360$
$2 * 2 * 8680$
$2 * 2 * 2 * 4340$
$2 * 2 * 2 * 2 * 2170$
$2 * 2 * 2 * 2 * 2 * 1085$
$2 * 2 * 2 * 2 * 2 * 5 * 217$
$2 * 2 * 2 * 2 * 2 * 5 * 7 * 31$

Therefore, the canonical form of 34720 is $2^5 * 5 * 7 * 31$.

3. Define congruence exactly as we defined it in class.

Let n be a positive integer
two integers a, b are said to be congruent modulo n written $a \equiv b\, mod(n)$
if $a - b = kn$ for some integer k

4. Suppose $n = 1! + 2! + 3! + ... + 100!$
Use congruence to find the remainder when n is divided by 12. This requires an argument, not a calculator. Show your work.

Let a be an integer where $a > 4$
As such, $a! = 1 * 2 * 3 * 4 * ... * a$

Thus $a\, mod(12) \equiv 0$ because $a!$ has factors 3 and 4 which have a product of 12 which shows that a is a multiple of 12

Now let $b,\ c$ be integers such that b and c are multiples of 12.
This means that b can be written as $12 * d$ and c can be written as $12 * e$ for some integers d, e
As such, $b + c = 12d + 12e$
$12d + 12e = 12(d + e)$
Thus, $(b + c)\, mod\, 12 \equiv 0$

By this reasoning, $(1! + 2! + 3! + ... + 100!)\, mod\, 12 \equiv (1! + 2! + 3! + 4!)\, mod\, 12 + 0$

Since $4!$ also contains factors 3 and 4 which have a product of 12, $4!\, mod\, (12) \equiv 0$ as well
Thus $(1! + 2! + 3! + 4!)\, mod\, 12 \equiv (1! + 2! + 3!)\, mod\, 12 \equiv (1 + 2 + 6)\, mod\, 12 \equiv 9$

Therefore, since $n\, mod(12) \equiv 9$, the remainder when n is divided by 12 is 9

5. Use Extended Euclid to prove Euclid's Lemma: if a|bc with a and b relatively prime, then a|c

From Extended Euclid, $gcd(a, b) = as + bt$.
Since a and b are relatively prime, $as + bt = 1$.
By multiplying both sides with c, $c = c(as + bt) = cas + cbt$.

The above lemma assumes $a|bc$, so we can say $a|cas$ and $a|cbt$.
Thus, $a|(cas + cbt)$ too.
Because $cas + cbt = c$, then $a|c$.

6. Prove that any two integers are congruent mod 1

Let a, b be integers.
1 is the smallest positive integer and any number divided by 1 leaves a remainder of 0.
Thus, a and b are congruent $mod\ 1$ for all a, b since their remainder when divided by 1 will always be equivalent (0).

7. Prove that any two integers are congruent mod 2 if both are even or both are odd

Let a belong to the set of positive integers and b belong to the set of negative integers.
$a = 2n$
$b = 2n + 1$
Isolating n in both equations, we get
$\frac{a}{2} = n$
$\frac{b}{2} = n + \frac{1}{2}$
If a is the set of negative integers and b is the set of positive integers, then a similar case is produced.
$a = 2n + 1 \ => \ \frac{a}{2} = n + \frac{1}{2}$

$b = 2n \ => \ \frac{b}{2} = n$
So, a and b cannot be equal if their signs are different.
Thus, any two integers can be congruent $mod\ 2$ only if $a, b > 0$ or if $a, b < 0$.

8. Prove the Modulus Addition Theorem

$Let\ x, y, p, n\ be\ integers\ with\ n > 0$
$if x \equiv y\ (mod\ n), then\ x \equiv (y + pn)\ (mod\ n)$

By definition of congruence, $x \equiv (y + pn)(mod\ n)$ shows that $x - (y + pn) = kn$ for some integer k
$x - (y + pn) = kn$
=> $x - (y) - pn = kn$
=> $x - (y) = kn + pn$
=> $x - (y) = n(k + p)$
Since (k + p) is the sum of two integers, (k + p) must also be an integer
As such, $x \equiv (y)(mod\ n)$

Therefore, if $x \equiv (y)(mod\ n)$, then $x \equiv (y + pn)(mod\ n)$ where x,y,p,n are integers with n > 0.

9. Use properties of congruence and the principle of mathematical inductions to show that for any positive integer, *k*,
$if\ a \equiv b\ (mod\ n)\ then\ a^k \equiv b^k\ (mod\ n)$

$k = 1$
So, $n|(a - b)$ such that $(a - b)\ mod\ n = 0.$
Thus, $a^1 - b^1 \equiv (a - b)(mod\ n)$ such that $a^1 \equiv b^1$.

$k = m + 1$
Assume $a^m \equiv b^m (mod\ n)$.
By induction, $a^{m+1} = a^m * a = b^m * b$.
By congruence, $(a - b)\ mod\ n = 0$.
As such, $(a^m * a - b^m * b)\ mod\ n\ => (a^m - b^m) * (a - b)\ \ (mod\ n = 0) * (mod\ n = 0)$
Therefore, $a^{m+1} \equiv b^{m+1} mod\ n$.

Thus, $a^k \equiv b^k (mod\ n)$ for any positive integer k.

10. Use the result from 9 (plus other properties of congruence) to show that 41 divides 2^{20} - 1

$2^5 mod(41) \equiv 32\ mod(41) \equiv\ - 9$
By the property proven in question 9, $(- 9)^2 \equiv 2^{10} mod(41)$
$81 \equiv 2^{10} mod(41)$

$81 + 1\, mod(41) \equiv 2^{10}\, mod(41) \; + \; 1 mod(41)$

$82 \equiv (2^{10} + 1)\, mod(41)$

$82 \; = \; 2 * 41$, so $82 mod(41) \equiv 0$

$(2^{10} + 1)\, mod(41) \equiv 0$

$(2^{10} - 1)(2^{10} + 1)\, mod(41) \equiv 0$

Therefore $(2^{20} - 1)\, mod(41) \equiv 0$