[redacted]

Project 3

Fun with Euclid & Congruence

Objectives

1. To practice with congruence properties
2. To develop skill in formal argumentation

Tasks

1. State the theorem that we called Extended Euclid.

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

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

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.

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

6. Prove that any two integers are congruent mod 1

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

8. Prove the Modulus Addition Theorem

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

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

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

Project Submission

Transform your LaTex (or very neatly written) work into a PDF file. Call it, project3.pdf
Submit it using GitHub. The instructions can be found by following links from the class website.

GitHub Classroom Accept Link: https://classroom.github.com/a/FJC3SZwv

1. Extended Euclid

Let a, b be integers with at least 1 of a, b non-zero.
then $\exists$ integers s, t

Such that
$$as + bt = \gcd(a, b)$$

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

2. $34720 = 2^5 \cdot 5 \cdot 7 \cdot 31$

3. Def Congruence
Two integers a, b are said to be congruent modulo n
(written $a \equiv b \pmod{n}$)
if $a - b = kn$ for some integer, k.

R

4. $n = 1! + 2! + 3! + \ldots + 100!$
Find $n \% 12$

$4! = 4 \cdot 3 \cdot 2 \cdot = 24$

$24 \equiv 0 \mod 12$

Any Term in n beyond 3 contains $4!$ as a factor

$n \equiv 1! + 2! + \ldots + 100! \equiv 1! + 2! + 3! \pmod{12}$

$\equiv 1 + 2 + 6 \pmod{12}$
$\equiv 9 \pmod{12}$

So $n \% 12 = 9$.

5. Euclid's Lemma
if $a | bc$ with a and b relatively prime then $a | c$
Since $\gcd(a, b) = 1$

by extended Euclid
$1 = as + bt$
$c = cas + cbt$
$= acs + bct$

$a \mid bc$ by assumption

$a \mid acs$ since $a \mid c$

$\Rightarrow a \mid (acs + bct)$

$a \mid c(as + bt)$

either $a \mid c$ or $a \mid (as+bt)$

but $(as+bt) = 1$
so $a \nmid (as+bt)$

So $a \mid c$ as claimed

6. any two integers are congruent mod 1.

pf

Let a, b be integers

Either $a = b$, $a > b$, or $b > a$

Case 1 $a = b$

$a - b = 0 \cdot 1$

$a \equiv b \mod 1$

Case 2

$a > b$

$a - b = k_1 \cdot 1$

$a \equiv b \mod 1$

Case 3

$b > a$

$b - a = k_2 \cdot 1$

$a \equiv b \mod 1$

7. Any two integers are congruent if both are even or both are odd

are

Case 1 a, b are even integers.

So $2 | a$ and $2 | b$

$a = 2k_1$, $b = 2k_2$ where k_1, k_2 are integers.

$a - b = 2k_1 - 2k_2$

$= 2(k_1 - k_2)$

$a \equiv b \mod 2$

Case 2 a, b are odd integers

So $a = k_1 + 1$
$b = k_2 + 1$
where k_1, k_2 are even.

$a - b = (k_1 + 1) - (k_2 + 1)$
$= k_1 - k_2$

Since k_1 and k_2 are even
they may be written

$k_1 = 2S$
$k_2 = 2T$

$(a - b) = 2S - 2T$
$= (S - T)2$

$a \equiv b \mod 2$

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

if $x \equiv y \pmod{n}$

$x \equiv (y + pn) \pmod{n}$

Pf

$x - y = kn$ def. of cong.

$x - y - pn = kn - pn$

$x - (y + pn) = (k - p)n$
where $k - p$ is an integer by the closure prop. of integers

$x \equiv (y + pn) \pmod{n}$ by the def. of cong.

9. Prove if $a \equiv b \pmod{n}$ $a^k \equiv b^k \pmod{n}$

By PMI

Base Case

$$a^1 \equiv b^1 \pmod{n}$$

Assume

$$a^m \equiv b^m \pmod{n} \text{ for some } m \geq 1$$

Show that this implies that

$$a^{m+1} \equiv b^{m+1} \pmod{n}$$

By the prop of cong.

if $p \equiv q \pmod{n}$ and $s \equiv t \pmod{n}$

Then $ps \equiv qt \pmod{n}$

Let $p = a^m$, $q = b^m$

$s = a$, $t = b$

Then

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

$$a^{m+1} \equiv b^{m+1} \pmod{n}$$

(as desired).

By PMI $a^k \equiv b^k \pmod{}$

$\forall k \geq 1$

10. Show $41 \mid 2^{20}-1$

$2^5 \equiv -9 \pmod{41}$

$(2^5)^4 \equiv (-9)^4 \pmod{41}$ prob. 9

$2^{20} \equiv 81 \cdot 81 \pmod{41}$

but $81 \equiv -1 \mod 41$

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

and $41 \mid 2^{20}-1$