Direct Proof of Part 2 Question 2

Should start with:

Let x be an arbitrary element that belongs to A. Our goal is to prove that x belongs to B.

Since x belongs to A, {x} belongs to P(A).

Since P(A) is a subset of P(B), {x} must belong to P(B).

By definition of power, all elements in any element of P(B), are elements of B. Thus, all elements of {x} belong to B, which means x belongs to B, as desired.

Number Theory - Proofs of Beginning principles

if $a \mid b$ and $b \mid c$, then $a \mid c$.

Goal is to find some integer x such that $c = ax$.

Since $a \mid b$, there exists an integer w, such that $b = aw$.

Since $b \mid c$, there exists an integer y, such that $c = by$.

$c = by = (aw)y = (wy)a$, since w and y are integers, their product is an integer, thus, we can conclude that $a \mid c$.

if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.

Since $a \mid b$, there exists an integer w, such that $b = aw$.

Since $b \mid a$, there exists an integer y, such that $a = by$.

$a = by = (aw)y = (wy)a$, where w and y are integers.

$a = (wy)\ a$

$1 = wy$, since w, y are ints, either both are 1 or both are -1.

Plug back in to get $a = b$ or $a = -b$

$5x + 10y$, since x and y are integers and we can factor out 5, we have:

$= 5(x + 2y)$, thus $5 \mid (5x + 10y)$.

But 5 does NOT evenly divide into 132.

Thus, there are no solutions.

If x and y are integers and $13 \mid (3x+4y)$,prove that $13 \mid (7x + 5y)$

Goal: express $7x + 5y$ as 13 times an integer.

$7x + 5y = 13x - 6x + 13y - 8y$

$= 13(x+y) - 2(3x+4y)$

$= 13(x+y) - 2(13c)$, since $13 \mid (3x+4y)$, for some integer c.

$= 13(x + y - 2c)$, since x, y and c are integers, so is $x + y - 2c$,

It follows that $13 \mid (7x + 5y)$

$7x + 5y = c(3x+4y) + (13n)x + (13m)y$, goal is to find some integers c, n and m that make this work.

$7 = 3c+13n$

$5 = 4c + 13m$

We don't want the 13s to bug us a lot, so a tool that will help us is mod.

Temporarily skipping: proof of infinite primes, division algorithm (will come back to)

<u>Mod Rules</u>

Definition of $a \equiv b \pmod{n}$ if and only if $n \mid (a-b)$.

$7 \equiv 3 \pmod{4}$

$13 \equiv -17 \pmod{30}$

$123456788 \equiv 8 \pmod{9}$ (Note: rule for divisibility by 9 is that whatever the Remainder is when you divide the sum of the digits of a number by 9 is the same remainder as when you divide the number by 9.)

Intuitively, mod just means both numbers leave the same remainder when divided by n, where n is the mod number. You can't do $n = 0$.

if $a \equiv b \pmod{n} \Leftrightarrow (a+c) \equiv (b+c) \pmod{n}$

if $a \equiv b \pmod{n} \Rightarrow ac \equiv bc \pmod{n}$

if $a \equiv b \pmod{n} \Rightarrow a^n \equiv b^n \pmod{n}$

if $a \equiv b \pmod{n} \Rightarrow f(a) \equiv f(b) \pmod{n}$ for any polynomial $f(x)$ with integer coefficients.

if $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

if $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$

if $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow ac \equiv bd \pmod{n}$

Example of Mod Proof

if $a \equiv b \pmod{n} \Rightarrow ac \equiv bc \pmod{n}$

Since $a \equiv b \pmod{n}$, it follows that $n \mid (b - a)$. This means there exists some integer x such that $b - a = nx$. Thus, $b = a + nx$.

Goal: to show that $n \mid (bc - ac)$.

$bc - ac = c(b - a)$
$= c(nx)$
$= n(cx)$, since c and x are integers, cx is an integer and we've proven that $n \mid (bc - ac)$.

$bc - ac = (a+nx)c - ac = ac + nxc - ac = n(cx)$, and we get to the same result.

One Cool Thing with Mod Rules
Modular Exponentiation…

Problem: Determine the remainder when 2^{123} is divided by 7.

2 x 2 x 2 x 2 … x 2 = ? mod 7

Note: result under column i is $2^i \equiv x \bmod 7$ (the one result, x, in between 0 and 6.)

Exp	0	1	2	3	4	5	6	7
Result	**1**	**2**	**4**	**1**	2	4	1	2

If $8 \equiv 1 \pmod 7$, then

$8(2) \equiv 1(2) \pmod 7$

$16 \equiv 2 \pmod 7$

$16(2) \equiv 2(2) \pmod 7$

EVERY TABLE LIKE THIS WILL EVENTUALLY REPEAT!!!

I could have stopped the table at 3.

Since 123 is divisible by 3, 2^{123} leaves a remainder of 1 when divided by 7.

2^{437} divided by 7 → 437 leaves a remainder of 2 when divided by 3, so the remainder when 2^{437} is divided by 7 is 4.

Fast Modular Exponentiation

Cycle method works well if the cycle is small!

But sometimes the cycles are not small.

Let's look at 2^{31} mod 19

Exp	0	1	2	4	8	16
Result	**1**	**2**	**4**	**16**	**9**	**5**

We know that $2^2 \equiv 4 \pmod{19}$

Instead of just going to 2^3, why not calculate 2^4:

$2^4 = (2^2)^2 = 4^2 = 4 \text{ x } 4 \equiv 16 \pmod{19}$

Use multiplication rule, but instead of multiplying by 2, multiply by 4.

$2^8 = (2^4)^2 = 16^2 \equiv (-3)^2 \pmod{19}$ because $16 \equiv -3 \pmod{19}$

$16 \text{ x } 16 \equiv -3 \text{ x } (-3) \pmod{19}$

$2^{16} = (2^8)^2 \equiv 9^2 = 81 \equiv 5 \pmod{19}$

$2^{31} = (2^{16})(2^8)(2^4)(2^2)(2^1) \equiv 5(9)(16)(4)(2) \equiv (45)(-3)(8) \equiv 7(-24) \equiv 7(-5) \equiv -35 \equiv 3 \pmod{19}$

The question what is the remainder when 2^{31} is divided by 19 is the same question as:

What is the unique integer x, with x >= 0 and x < 19 such that

$2^{31} \equiv x \pmod{19}$?