

DISCRETE MATHEMATICS
HOMEWORK 9

1. Solve simultaneously the congruences

$$x \equiv 5 \pmod{21}$$

$$x \equiv 7 \pmod{92}$$

$$x \equiv 2 \pmod{5}.$$

2. Compute the sums

$$1$$

$$1 + 3$$

$$1 + 3 + 5$$

$$1 + 3 + 5 + 7$$

etc.

until you see a pattern. Can you convince me of the truth of this pattern?

3. Compute the sums

$$2^0$$

$$2^0 + 2^1$$

$$2^0 + 2^1 + 2^2$$

$$2^0 + 2^1 + 2^2 + 2^3$$

etc.

until you see a pattern. Can you convince me of the truth of this pattern?

4. Use Fermat's test to convince me that 39 is not a prime. (Let me be clear: I'd really like to use the Fermat test, even though it is not the quickest way to see that 39 is composite.)
5. In class, we used the following proposition while proving Fermat's Little Theorem:

Theorem. *p is a prime if and only if every $a \neq 0 \in \mathbb{Z}_p$ has a multiplicative inverse $1/a$ in \mathbb{Z}_p .*

Explain what this result means, and why it is true.

6. We've looked at a lot of examples of solving pairs of congruences. Try to pull together what we've learned by proving the *Chinese Remainder Theorem*:

Theorem. *The system of congruences*

$$x \equiv a \pmod{m}$$

$$x \equiv b \pmod{n}$$

has exactly one solution mod mn as long as $\gcd(m, n) = 1$.

Can you explain what happens when $\gcd(m, n) > 1$? *Remark:* I'd do this by turning the pair of congruences into a Diophantine equation, and using stuff about the solutions of the Diophantine equation.

7. Using among other things the theorem that if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$, try to construct an argument that every positive integer factors into primes in exactly one way. This argument will have two parts.
- (a) First, prove that every integer factors into primes.
 - (b) Then prove that if

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$$

are two factorizations of a into primes, then $n = m$ and the primes p_1, p_2, \dots, p_n are a rearrangement of the primes q_1, q_2, \dots, q_m . It is this second part of the proof that will need the theorem mentioned above.