

2nd Midterm
Math 2770
22 June 2004
Dr. Michael Oliver

NAME: _____

1) Let $a, c, d \in \mathbb{Z}$, and suppose $a|d$, $c|d$, but $a \nmid c$ (this last is to be read “ a does *not* divide c ”). Does a divide $c + 2d$? Choose one of the following and follow the instructions:

- a) Yes, always (you must prove it)
- b) No, never (you must prove it)
- c) Sometimes yes and sometimes no (you must find values of a, c, d , satisfying the conditions, for which the answer is “yes”, and other values for which the answer is “no”).

2)

- a) Use Euclid's Algorithm to find $\gcd(5, 17)$. At each stage, keep track of what linear combination of 5 and 17 is each of the numbers x_i, y_i that occurs.

- b) Does 5 have a multiplicative inverse modulo 17? (I.e. is there a number n such that $5n \equiv 1 \pmod{17}$?) If so, what is it? If not, how can you tell?

(Note—this is easy to do in your head, but for full credit show how the answer comes out of the answer to part (a).)

3) Prove the “existence” part of the Fundamental Theorem of Arithmetic; that is, prove that every natural number greater than 1 has a prime factorization. I.e., you want to show that there isn’t some huge n with the property that, no matter how you multiply primes together, you can never obtain exactly n . Use either strong induction or the method of infinite descent. It is not necessary to be extremely formal, but you must show how induction or infinite descent is used.

4)

a) Find an integer x such that

$$\begin{aligned}x &\equiv 1 \pmod{5} \\x &\equiv 2 \pmod{17}\end{aligned}$$

For full credit, this should be done in a way that follows the proof of the Chinese Remainder Theorem, except that to save time you may find multiplicative inverses in your head rather than calculating them via Euclid's Algorithm. Also look back at problem 2 to see if you've already calculated one of the multiplicative inverses you need.

b) (Extra credit==1/2 problem) Suppose we add to the two congruences in part (a) the extra condition

$$x \equiv 6 \pmod{10}$$

Now does the system of congruences have a solution? If so, find one; if not, explain why.

5) Recall that $\phi(n)$, the Euler totient function, is defined as the number of natural numbers less than n that are relatively prime to n .

a) What is the value of $\phi(45)$?

b) What is the value of $7^{24,000,002} \pmod{45}$? Hint: Apply part (a) and the extended Fermat's Little Theorem, and then do just a little more work after that (do you remember your laws of exponents?)