ASSIGNMENT 2: NUMBER THEORY CONTINUED!

OCTOBER 4, 2020

Euclid's algorithm revisited

Recall the following simple statement.

If a, b are positive integers, with $a \geq b$, then

- Pairs (a, b) and $(a - b, b)$ have same common divisors (i.e., d is a common divisor of (a, b) if and only if it is a common divisor of $(a - b, b)$)
- Let r be the remainder upon division of a by b: $a = bq + r$. Then pairs (a, b) and (b, r) have the same common divisors.

This implies the Euclid algorithm of finding the greatest common divisor of (a, b): start with pair (a, b) and replace it by $(b, r = a \mod b)$; repeat until you have pair $(d, 0)$. The gcd doesn't change during this, so $\gcd(a, b) = \gcd(d, 0) = d$.

This also implies more useful corollaries.

1. A number n is a common divisor of (a, b) if and only if n is a divisor of $d = \gcd(a, b)$.
2. A number c can be written as a combination of a, b (i.e. in the form $ax + by$, with x, y integer) if and ony if c is a multiple of $d = \gcd(a, b)$.

Problems

1. Find a 6-digit number such that when you multiply it by 2, 3, 4, 5, 6, you again get a 6-digit number with the same digits, but in different order.

2. (Many of you already know this, but if you never seen it before, please try doing this).
   Show that number a is invertible mod n (i.e. there exists an integer x such that $ax \equiv 1 \mod n$) if and only if $\gcd(a, n) = 1$); in this case, numbers a, n are called *relatively prime*.
   [Hint: look at corollary 2 above.]

3. What is the largest integer that can not be written in the form $17x + 39y$ with non-negative integer x, y?

4. (a) Let $a > b$ be positive integers. Show that then
   $$\gcd(2^a - 1, 2^b - 1) = \gcd(2^{a-b} - 1, 2^b - 1)$$
   (b) Show that
   $$\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1.$$
   (c) Does the same work if we replace 2 by other numbers?

5. (a) Show that $2^{3k} + 1$ is divisible by $2^k + 1$
   (b) Show that the same is true if we replace 3 by any odd integer: e.g., $2^{5k} + 1$ is also divisible by $2^k + 1$
   (c) Show that if a number $2^m + 1$ is a prime, then m itself is a power of 2.
   (d) Find as many prime numbers of the form $2^m + 1$ as you can. Whoever gets most, gets a special prize!

Harder problems

Five men and a monkey were shipwrecked on an island. They spent the first night gathering coconuts. During the night, one man woke up and decided to take his share of the coconuts. He divided them into five piles. One coconut was left over so he gave it to the monkey, then hid his share, put the rest back together, and went back to sleep.

Soon a second man woke up and did the same thing. After dividing the coconuts into five piles, one coconut was left over which he gave to the monkey. He then hid his share, put the rest back together, and went back to bed. The third, fourth, and fifth man followed exactly the same procedure.

The next morning, after they all woke up, they divided the remaining coconuts into five equal shares; again, one coconut was left over so they gave it to the monkey.
How many coconuts were there in the original pile?

[An alternative, slightly more difficult version of this problem is that on the final morning, there was no coconut left over to give to the monkey.]