JUNE 14TH MATH PROBLEM SET

Therefore, we should take great care not to accept as true such properties of the numbers which we have discovered by observation and which are supported by induction alone. – Leonhard Euler

Consider a number n (such as $n = 15$). A natural question is

How many integers are there, between 1 and n, which are relatively prime to n?

The answer to this question is denoted by $\phi(n)$. The function ϕ is called *Euler's ϕ function.*

1. For each of the following numbers N, compute $\phi(n)$. Divide up the work among people in your group. The first group to finish get's a point.

(a) 10
(b) 9
(c) 11
(d) 37
(e) 15
(f) 45
(g) 22
(h) 27
(i) 30
(j) 32
(k) 49
(l) 50

2. Make some general predictions about what $\phi(n)$ is. At least for special kinds of n. Some particular cases to consider. You don't have to answer all of them.

(a) What if n is prime.
(b) What if $n = 2p$ for p prime?
(c) What if $n = p^2$ for p prime?
(d) What if $n = p^3$ for p prime?
(e) What if $n = p^n$ for p prime?
(f) What if $n = pq$ for p and q different, but both prime?

Put your predictions on the board.

3. Try to find a general algorithm for computing $\phi(n)$. Write your group's prediction on the board.

There is a famous theorem in number theory called the *Chinese Remainder Theorem*. It says the following.

Theorem. *Suppose n, m are relatively prime with* $\gcd(n, m) = 1$. *Then for any integers a, b, there is a solution to the system equations:*

$$\begin{aligned} x &\equiv_n a \\ x &\equiv_m b. \end{aligned}$$

4. Show that the theorem is true. In particular, find x.

Hint: Write $1 = sn + tm$ for some integers s and t. Now multiply through by a and mod out by n. Likewise multiply by b and mod out by m. Combine these observations in a clever way.

5. Suppose $\gcd(n, m) = 1$. Also suppose that both

$$\begin{aligned} x &\equiv_n a \\ x &\equiv_m b \end{aligned}$$

and

$$\begin{aligned} y &\equiv_n a \\ y &\equiv_m b. \end{aligned}$$

for some integers x, y. Show that nm divides $x - y$ or in other words that $x \equiv_{nm} y$.

Hint: We know that $x \equiv_n a \equiv_n y$. So n divides $x - y$. Use the fact that n and m are relatively prime.

6. Suppose that $\gcd(n, m) = 1$ and that

$$\begin{aligned} x &\equiv_n a \\ x &\equiv_m b. \end{aligned}$$

If $x \equiv_{nm} y$, show that we also have that

$$\begin{aligned} y &\equiv_n a \\ y &\equiv_m b. \end{aligned}$$

Hint: We know that $x + k(nm) = y$ for some integer k.

Problems 5 and 6 can be combined with our first version of the Chinese remainder theorem to say that:

Theorem. *Suppose n, m are relatively prime with $\gcd(n, m) = 1$. Then for any integers a, b, there is a solution to the system equations:*

$$\begin{aligned} x &\equiv_n a \\ x &\equiv_m b. \end{aligned}$$

Furthermore, if y is a solution, then z is another solution if and only if $y \equiv_{nm} z$.

7. Keep assuming $\gcd(n, m) = 1$. Suppose I have an integer y between 0 and $nm - 1$. I can consider two remainders $r_1 = y (\text{mod } n)$ and $r_2 = y (\text{mod } m)$. Show two things.

(i) If y is relatively prime to nm, then r_1 is relatively prime to n and r_2 is relatively prime to m.

(ii) If r_1 is relatively prime to n and r_2 is relatively prime to m then y is relatively prime to nm.

Hint: For (i), suppose a prime number $p > 1$ divides r_1 and n. Since $y = q_1 n + r_1$, conclude that p also divides y. For (ii) suppose a prime number p divides both y and nm.

8. Use this new version of the Chinese remainder theorem, when combined with problem 7 to precisely find a formula for $\phi(nm)$ in terms of $\phi(n)$ and $\phi(m)$ when n and m are relatively prime.

Hint: The following is a good way to think about it. Consider the numbers $0, 1, 2, \ldots, nm - 1$. For each such number, we get two remainders r_1 and r_2 modulo n and m respectively. The Chinese remainder theorem says that each pair of remainders is hit exactly once by a number in $0, 1, 2, \ldots, nm - 1$. Count the ones that are relatively prime to nm.