JUNE 9TH MODULAR ARITHMETIC PROBLEM SET

Can you do Division? Divide a loaf by a knife - what's the answer to that? – Lewis Carroll

Today we are going to learn an algorithm for finding gcd's (greatest common divisors). One amazing result of this algorithm is that it also will tell us how to invert a modulo n if $\gcd(a, n) = 1$.

First we need to relearn division.

Definition. Given two integers a and $b > 0$, we can always write $a = qb + r$ where $0 \leq r < b$. The number q is called the quotient, the number r is called the remainder.

This is something I assume you already know, just written in a more formal way.

1. Find the q and the r for the following choices of a and b.

(i) $a = 15$, $b = 7$.

(ii) $a = 8$, $b = 1$

(iii) $a = -10$, $b = 4$

(iv) $a = 22$, $b = 11$

We say that b *divides* a *if when writing* q *and* r *above,* $r = 0$. That is, we say that b divides a if a/b has no remainder.

The strategy we will use to find gcds relies on the following fact.

$$\gcd(a, b) \text{ is the same as } \gcd(a, b + a)$$

2. Let's show that they are equal.

(i) Let $d = \gcd(a, b)$. See if you can explain why d divides $b + a$ evenly. A good way to do it is to write $a = qd$ and $b = q'd$. Then add those two equations together.

(ii) On the other hand if $e = \gcd(a, b + a)$, explain why e divides a evenly.

(iii) Now conclude that $d = e$.

Hint: From (i), we know that d divides a and $b + a$. Hence d divides $\gcd(a, b) = e$ (you can use this without proof). Now reverse the process.

3. Convince yourself, as a group, that $\gcd(a, b) = \gcd(a, b + ka)$ for any integer k (positive or negative).

Here comes the algorithm.

Algorithm: Given two numbers a, b, if $a = b$ then $\gcd(a, b) = a$ and we are done. Likewise if $a = 0$, then $\gcd(a, b) = b$ or if $b = 0$, then $\gcd(a, b) = a$. Otherwise one number is bigger. Let's call that one a. Write $a = bq + r$ with $0 \leq r < b$. Then

$$\gcd(a, b) = \gcd(r, b)$$

so compute $\gcd(r, b)$. Keep going like this until you end up computing $\gcd(a, b)$. Note the numbers get smaller with each step.

4. Use this algorithm to compute the gcds of the following pairs of numbers:

(i) 25, 49

(ii) 221, 187

(iii) 91, 247

(iv) 253, 161

Let's work through one example. $\gcd(63 = a, 49 = b)$. $63 = q_1 49 + r_1$ where $q_1 = 1$ and so $r_1 = 14$. Next we compute $\gcd(49, 14 = r_1)$, write $49 = q_2 14 + r_2$ where $q_2 = 3$, $r_2 = 7$. Next we compute $\gcd(14 = r_1, 7 = r_2)$. Finally we write $14 = q_3 7 + r_3$ with $q_3 = 2$ and $r_3 = 0$. Now we stop since next we compute $\gcd(7, 0) = 7$. Let's reverse the steps now.

$7 = r_2 = (49 - q_2 14) = (b - q_2 r_1) = b - q_2(63 - q_1 49) = b - q_2(a - q_1 b) = (q_1 q_2 + 1)b + (-q_2)a = 2b + (-3)a.$

Notice this really is right, $4 \cdot 49 - 3 \cdot 63 = 196 - 189 = 7$. Something like this always works. It means that

$$\gcd(a, b) = sa + tb$$

for some appropriately chosen integers s, t. We'll work on implementing this next week. But for now, let's just see what it's good for right now.

5. For the following pairs of numbers below, $\gcd(a, b) = 1$. Find integers s and t with $sa + tb = 1$. You can use the Euclidean algorithm or just guess and check.

(i) 5, 7

(ii) 9, 16

(iii) 15, 49

(iv) 10, 37

6. For each s,t pair you found in 5., show that s is the inverse of a modulo b. In other words, show that $sa \equiv_b 1$. *Hint:* For example, let me do the first one for you. Say $a = 5$, $b = 7$. Choose $s = 3$, $t = -2$. Then $sa + tb = 3 \cdot 5 + (-2) \cdot 7 = 15 - 14 = 1$. We need to verify that $s \cdot a \equiv_b 1$. So let's do it.

$$3 \cdot 5 = 15 \equiv_7 1.$$

There, we did (i).

7. Verify in general that if $sa + tb = 1$, then $sa \equiv_b 1$.