A BIT MORE EUCLID, THEN SOME EULER

MATH CIRCLE (BEGINNERS) 03/04/2012

The **Extended Euclidean Algorithm** is a way to solve equations of the form

$$ax + by = c,$$

where a, b, c are known integers, and you're looking for integer values of x and y that make the equation true (assuming they exist!).

Remember the ordinary Euclidean algorithm? Here's a reminder of the process, along with a specific example to refresh your memory:

$$\begin{aligned}
a &= q_1 b &+ r_1 &\qquad (0 < r_1 < b)\\
b &= q_2 r_1 &+ r_2 &\qquad (0 < r_2 < r_1)\\
r_1 &= q_3 r_2 &+ r_3 &\qquad (0 < r_3 < r_2)\\
r_2 &= q_4 r_3 &+ r_4 &\qquad (0 < r_4 < r_3)\\
&\vdots\\
r_{n-2} &= q_n r_{n-1} &+ r_n &\qquad (0 < r_n < r_{n-1})\\
r_{n-1} &= q_{n+1} r_n &+ 0
\end{aligned}$$

Example: Find $\gcd(76, 32)$ (so in this case $a = 76$, $b = 32$):

$$\begin{aligned}
76 &= 2 \cdot 32 &+ 12\\
32 &= 2 \cdot 12 &+ 8\\
12 &= 1 \cdot 8 &+ 4\\
8 &= 2 \cdot 4 &+ 0
\end{aligned}$$

Now that we've done that, we can use the **Extended** Euclidean Algorithm to find x and y such that $ax+by = gcd(a, b)$. In this particular case: $76x+32y = 4$. The way to do it is to use the results from the ordinary Euclidean Algorithm, but to work backwards from the next-to-last line. To make things easier on us, let's start by rewriting the equations in an equivalent way, namely with the remainders by themselves on the left side:

$$\begin{aligned}
76 &= 2\cdot 32 + 12 \quad \rightarrow \quad 12 = 76 + (-2)\cdot 32 \qquad (\#1)\\
32 &= 2\cdot 12 + 8 \quad \rightarrow \quad 8 = 32 + (-2)\cdot 12 \qquad (\#2)\\
12 &= 1\cdot 8 + 4 \quad \rightarrow \quad 4 = 12 + (-1)\cdot 8 \qquad (\#3)\\
8 &= 2\cdot 4 + 0
\end{aligned}$$

Since equation #2 tells us that $8 = 32 + (-2)\cdot 12$, we can substitute $32 + (-2)\cdot 12$ into equation #3 in place of 8. So equation #3 becomes

$$4 = 12 + (-1)\cdot(32 + (-2)\cdot 12)$$

Combining the 12's and 32's gives:

$$4 = 12 + (-1)\cdot 32 + 2\cdot 12$$

$$4 = (-1)\cdot 32 + 3\cdot 12 \qquad (\#4)$$

I called this new equation Equation #4. But look: Equation #1 tells us that $12 = 76 + (-2)\cdot 32$, so we can substitute $76 + (-2)\cdot 32$ into equation #4 now in place of 12. Excellent! Equation #4 becomes

$$\begin{aligned}
4 &= (-1)\cdot 32 + 3\cdot(76 + (-2)\cdot 32)\\
4 &= (-1)\cdot 32 + 3\cdot 76 + (-6)\cdot 32
\end{aligned}$$

$$4 = 3\cdot 76 + (-7)\cdot 32$$

And we are done! This tells us that to solve $76x + 32y = 4$, we can take $x = 3$, $y = -7$. Hooray!!! See if you can use the Extended Euclidean Algorithm to solve the following equations:

(1) $11x + 7y = 1$

(2) $25x + 35y = 5$

(3) $16x + 7y = 3$

(Hint: First solve $16x + 7y = 1$**. Then what?)**

(4) $16x + 58y = 2$

We can use the Extended Euclidean Algorithm to compute inverses in modular arithmetic. Remember the (multiplicative) inverse of a number $\pmod n$ is the number you multiply it to get $1 \pmod n$. So for example, 5 and 3 are inverses of each other $\pmod 7$, because $5 \cdot 3 \equiv 1 \pmod 7$, and 5 is its own inverse $\pmod 8$, because $5 \cdot 5 \equiv 1 \pmod{\{}8\}$.

When we're looking for an inverse to $a \pmod n$, we want a number x so that $a \cdot x \equiv 1 \pmod n$. This means that the remainder when you divide $a \cdot x$ by n is 1, or in other words $a \cdot x = y \cdot n + 1$ for some unknown y.

But another way to write that equation is

$$a \cdot x - n \cdot y = 1.$$

The numbers we know are a and n, and the Extended Euclidean Algorithm lets us solve this to find an x and y that work...

For instance, if I wanted to find the inverse of $14 \pmod{31}$, I would use EEA to solve $14x - 31y = 1$, and then whatever I get for x is the inverse of 14.

(5) What is the inverse of $14 \pmod{31}$? (Use the Extended Euclidean Algorithm)

(6) What is the inverse of $11 \pmod{100}$**?**

(7) What is the inverse of $7 \pmod{72}$**?**

Two numbers are *relatively prime* if they share no prime factors with each other. This means they can't have any common divisors other than 1, so their gcd must be 1. On the other hand, if their gcd is 1, they don't have any common divisors other than 1, so they don't share any prime factors, so they are relatively prime:

Fact: x and y have no prime factors in common if and only if $\gcd(x, y) = 1$.

(8) For each pair of numbers, decide whether they are relatively prime (YES or NO):

(a) 17 and 6

(b) 74 and 60

(c) 11 and 111

(d) 56 and 45

(e) 39 and 18

(f) 42 and 91

(g) 105 and 88

(h) 13 and 117

The Greek letter ϕ is written "phi" and pronounced "fee." The mathematician Euler used it to describe how many numbers less than a certain number, were relatively prime to that number. Nowadays we call this number the *Euler phi function*.

$\phi(n) =$**the number of numbers between** 1 **and** $n-1$**, that are relatively prime to** n**.**

For example, $\phi(10) = 4$, because there are 4 numbers less than 10 that are relatively prime to 10 (1, 3, 7, and 9). The other numbers less than 10 (2, 4, 5, 6, and 8) all share a prime factor with 10.

(9) Fill in this table with the value of $\phi(n)$ for n from 2 to 21 (we've started you out with the first few):

n	2	3	4	5	6	7	8	9	10	11
$\phi(n)$	1	2	2						4	

n	12	13	14	15	16	17	18	19	20	21
$\phi(n)$										

(10) What is the value of $\phi(p)$ when p is a prime number?

(11) What is the value of $\phi(1024)$? (Hint 1: $1024 = 2^{10}$.) (Hint 2: Look for a pattern with $\phi(2)$, $\phi(4)$, $\phi(8)$, $\phi(16)$, ...)

(12) Sometimes $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$–for example, $\phi(3 \cdot 5) = \phi(15) = 8$, and also $\phi(3) = 2$, $\phi(5) = 4$, and $8 = 2 \cdot 4$.

Other times this doesn't work: $\phi(2 \cdot 4) = \phi(8) = 4$, but $\phi(2) = 1$ and $\phi(4) = 2$ and $4 \neq 1 \cdot 2$.

Let's call a pair of numbers a and b a *happy couple* if $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$. Find the values $\phi(a \cdot b)$, $\phi(a)$, and $\phi(b)$ for several pairs of numbers a and b (at least 4 different pairs–you don't have to compute them from nothing, since you have the table you made above). Make a list of which ones are happy couples and which ones aren't. Compare lists with your neighbors. Try to find an underlying pattern–when is a pair of numbers a happy couple?