

1. Extended Euclidean Algorithm

2. Congruence notation

MATH2068 Number Theory & Cryptography
Week 3 Lecture 1

University of Sydney
NSW 2006
Australia

4th August 2008



The extended Euclidean Algorithm

Problem: Use the E.E.A. to show that $\gcd(136, 60) = 4$ and find $s, t \in \mathbb{Z}$ with $136s + 60t = 4$.

Solution:

A	B	136	60	16	12	4	0
	Q			2	3	1	3
L	K	0	1	2	7	9	34
N	M	1	0	1	3	4	15

$$136 = 2 \times 60 + 16 \quad 2 \times 1 + 0 = 2 \quad 2 \times 0 + 1 = 1$$

$$60 = 3 \times 16 + 12 \quad 3 \times 2 + 1 = 7 \quad 3 \times 1 + 0 = 3$$

$$16 = 1 \times 12 + 4 \quad 1 \times 7 + 2 = 9 \quad 1 \times 3 + 1 = 4$$

$$12 = 3 \times 4 + 0 \quad 3 \times 9 + 7 = 34 \quad 3 \times 4 + 3 = 15$$

The final values of A , L and N are the numbers we want:

$$\gcd(136, 60) = A = 4,$$

$$4 = 136N + 60(-L) = 136 \times 4 - 60 \times 9.$$

Why does it work?



We make a table that looks like this:

a	b	A	B	R
					Q
0	1	L	K	$QK + L$
1	0	N	M	$QM + N$

Initially $A = a$, $B = b$ and $(L, K, N, M) = (0, 1, 1, 0)$.

The equations $a = AK + BL$ and $b = AM + BN$ hold.

Now we put $A = QB + R$, and so

$$a = (QB + R)K + BL = B(QK + L) + RK = A'K' + B'L'$$

$$b = (QB + R)M + BN = B(QM + N) + RM = A'M' + B'N'$$

where A' , B' etc. are the new values of A , B etc..

So the equations in blue stay true all the way through.

Explanation continued



Similarly we can show that $LM - NK = \pm 1$ always holds.

(The sign changes at each step).

At the end we have $A = d$ (the gcd) and $B = 0$

$$a \quad b \quad \dots \quad d \quad 0$$

$$0 \quad 1 \quad \dots \quad L \quad K$$

$$1 \quad 0 \quad \dots \quad N \quad M$$

and so $a = dK + 0L = dK$ and $b = dM + 0N$.

That is, $K = (a/d)$ and $M = (b/d)$.

So $LM - NK = \pm 1$ becomes $L(b/d) - N(a/d) = \pm 1$.

Hence $Lb - Na = \pm d$.

E.E.A. example continued



Problem: Find, if possible, $s, t \in \mathbb{Z}$ with $136s + 60t = 20$.

Solution: We have just seen that $136 \times 4 - 60 \times 9 = 4$.
Since $4 \mid 20$, there is no problem! Just multiply through by 5.

$$136 \times 20 - 60 \times 45 = 20. \quad (\text{So } s = 20, t = -45 \text{ will do.})$$

Problem: Find, if possible, $s, t \in \mathbb{Z}$ with $136s + 60t = 26$.

Solution: We have seen that $\gcd(136, 60) = 4$.
Since $4 \nmid 26$, there is a big problem!
For all values of s, t it is the case that $4 \mid (136s + 60t)$.
So $136s + 60t = 26$ has no solution.

Conclusion: Given $a, b, m \in \mathbb{Z}$, there exist $s, t \in \mathbb{Z}$ such that $sa + tb = m$ if and only if $\gcd(a, b) \mid m$.

E.E.A. example continued some more



Problem: Find all $s, t \in \mathbb{Z}$ such that $136s + 60t = 20$.

Solution: We have seen that $(s_0, t_0) = (20, -45)$ is one solution.

Now (s, t) is another solution iff $136s + 60t = 136s_0 + 60t_0$.

Equivalently, $136(s - s_0) = 60(t_0 - t)$.

Dividing by $\gcd(136, 60) = 4$ gives $34(s - s_0) = 15(t_0 - t)$.

Solution: put $s - s_0 = 15k$ and $t_0 - t = 34k$, for any $k \in \mathbb{Z}$.

So $(s, t) = (s_0 + 15k, t_0 - 34k)$ is a solution for all $k \in \mathbb{Z}$.

Later we will see that these are the only possible solutions.

Conclusion: Given $a, b, m \in \mathbb{Z}$ such that $d = \gcd(a, b)$ is a divisor of m , the general solution of $sa + tb = m$ is

$$s = s_0 + (b/d)k$$

$$t = t_0 - (a/d)k$$

where (s_0, t_0) is a particular solution (found by E.E.A.), and $k \in \mathbb{Z}$ is arbitrary.

Another E.E.A. example



Problem: Find all $s, t \in \mathbb{Z}$ such that $182s + 49t = 4$.

$$\begin{array}{cccccc} 182 & 49 & 35 & 14 & 7 & 0 \\ & & & 3 & 1 & 2 & 2 \\ 0 & 1 & 3 & 4 & 11 & 26 \\ 1 & 0 & 1 & 1 & 3 & 8 \end{array}$$

The gcd is 7, and $7 \nmid 4$. So $182s + 49t = 4$ has no integer solutions.

Problem: Find all $s, t \in \mathbb{Z}$ such that $182s + 49t = 77$.

It's OK now since $7 \mid 77$.

From the E.E.A. (2nd last column), $182 \times 3 + 49 \times (-11) = 7$.

Multiply by 11: $182 \times 33 + 49 \times (-121) = 77$.

Now $\gcd(182, 49) = 7$, and we have $\frac{49}{7} = 7$ and $\frac{182}{7} = 26$.

Solution: $182 \times (33 + 7k) + 49 \times (-121 - 26k) = 77$ for all k .

A few definitions



If $a, b \in \mathbb{Z}$ then " $b \mid a$ " means " $a = qb$ for some $q \in \mathbb{Z}$ ".

Now $a = qb$ and $-a = (-q)b$ are equivalent to each other, and also to $a = (-q)(-b)$ and $-a = q(-b)$.

So $b \mid a$ iff $\pm b \mid \pm a$, for any and all choices of the signs.

If $a, b \in \mathbb{Z}$ with $b > 0$ we have defined the residue of a modulo b to be the integer $r = a - qb$ satisfying $0 \leq r < b$.

When $b < 0$ we define the residue of a modulo b to be the same as the residue of a modulo $|b|$.

If m, n are integers, possibly negative, we define $\gcd(m, n)$ to be the same as $\gcd(|m|, |n|)$.

Definition: Integers m, n are said to be *coprime* or *relatively prime* if $\gcd(m, n) = 1$.

Congruence notation



Definition: Let $n \in \mathbb{Z}$. We say that integers a, b are *congruent modulo n* if $a - b = kn$ for some $k \in \mathbb{Z}$.

We write " $a \equiv b \pmod{n}$ " for " a is congruent to b modulo n ".

So $a \equiv b \pmod{n}$ if and only if $a - b = kn$ for some $k \in \mathbb{Z}$.

e.g. $12 \equiv (-9) \pmod{7}$ since $12 - (-9) = 21$ is a multiple of 7.

If $n \neq 0$ then $a \equiv b \pmod{n}$ if and only if a and b have the same residue modulo n .

e.g. 16 and 51 both have residue 1 mod 5; so $16 \equiv 51 \pmod{5}$.

Why is congruence notation useful?



Because of the following theorem:

Theorem: If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ then $a + b \equiv a' + b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

"Addition and multiplication respect congruence".

Proof: $a \equiv a' \pmod{n}$ gives $a' = a + kn$ for some $k \in \mathbb{Z}$.

And $b \equiv b' \pmod{n}$ gives $b' = b + hn$ for some h .

Adding these gives $a' + b' = a + b + (k + h)n$.

So $a + b \equiv a' + b' \pmod{n}$.

Similarly, multiplying the equations above gives

$$a'b' = (a + kn)(b + hn) = ab + (kb + ah + khn)n$$

giving $ab \equiv a'b' \pmod{n}$.

Congruence examples



(1) Since 22 and 31 differ by 9, we have $22 \equiv 31 \pmod{9}$.

And 53 and 35 differ by 18; so $53 \equiv 35 \pmod{9}$.

Hence $22 \times 53 \equiv 31 \times 35 \pmod{9}$.

Check: $22 \times 53 = 1166$ and $31 \times 35 = 1085$.

These differ by 81, a multiple of 9.

(2) Since $7|28$ it follows that $27 \equiv -1 \pmod{7}$.

So $27^{101} - 3 \equiv (-1)^{101} - 3 \equiv -1 - 3 \equiv 3 \pmod{7}$.

(3) **Problem:** Find the residue of 68^{1000} modulo 13.

Solution: $13|65$; so $68 \equiv 3 \pmod{13}$.

Now $3^3 = 27 \equiv 1 \pmod{13}$. So $68^{1000} \equiv 3^{1000} \equiv 3^{999} \times 3$, and $3^{999} = (3^3)^{333} \equiv 1^{333} \equiv 1$. So $68^{1000} \equiv 3 \pmod{13}$.

The residue is 3.

Solving a congruence



Problem: Find, if possible, an $s \in \mathbb{Z}$ with $68s \equiv 1 \pmod{21}$.

Solution: We want $68s - 1 = 21t$ for some t .

That is, $68s - 21t = 1$.

We have just been doing problems like this!

$$\begin{array}{cccccc} 68 & 21 & 5 & 1 & 0 & \\ & & 3 & 4 & 5 & \\ & 0 & 1 & 3 & 13 & \\ & 1 & 0 & 1 & 4 & \end{array}$$

The gcd is 1; so there is a solution.

And indeed $68 \times (-4) + 21 \times 13 = 1$.

So $68 \times (-4) \equiv 1 \pmod{21}$.

A basic theorem



Theorem: Suppose that $a, b, n \in \mathbb{Z}$ and $n|ab$.
If $\gcd(n, a) = 1$ then $n|b$.

Proof: Since $\gcd(n, a) = 1$ there exist $s, t \in \mathbb{Z}$ with $sa + nt = 1$.
Multiplying through by b gives $sab + NTB = b$.
Since $n|ab$ both terms on LHS are multiples of n .
So $n|b$.

Example: $77 \times 663 = 51051 = 51 \times 1001$.

But $\gcd(51, 77) = 1$. So $51|663$.

(However, $21|(77 \times 663)$ even though $21 \nmid 77$ and $21 \nmid 663$.)

And an important corollary



Corollary: Let $a, b, p \in \mathbb{Z}^+$ and suppose that p is prime.
If $p|ab$ then $p|a$ or $p|b$.

Proof: Let $d = \gcd(p, a)$. Then $d|p$; so either $d = 1$ or $d = p$.
(Since p prime it has no other divisors.)

Case 1: If $d = 1$ then we have $p|ab$ and $\gcd(p, a) = 1$.

By the theorem it follows that $p|b$.

Case 2: Suppose that $d = p$.

Since $d = \gcd(p, a)$ we have that $d|a$.

That is, $p|a$, as required.