Sep-8

Extended EA (EEA)

Using EA to find x, y s.t. $1 = ax + by$ is tedious. Requires a forward pass and a backwards pass.

EEA adds an extra step to each iteration, which eliminates the need for the backwards pass.

In each step, we compute ① $s_j = s_{j-2} - q_{j-1} s_{j-1}$

② $t_j = t_{j-2} - q_{j-1} t_{j-1}$

We define $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$

$\gcd(1205, 37)$:

$s_2 = s_0 - q_1 \cdot s_1$

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	1205	37	32	21	1	0
1	37	21	1	16	0	1
2	21	16	1	5	$1-(32)(0)=1$	$0-(32)(1) = -32$
3	16	5	3	1	$0-(1)(1)=-1$	$1-(1)(-32) = 33$
4	5	1	5	0	$1-(1)(-1)=2$	$-32-(1)(33) = -65$
5					$-1-(3)(2)=-7$	$33-(3)(-65) = 228$

$$1 = 1205(-7) + 37(228)$$

$$\gcd(a,b) = a(s_\ell) + b(t_\ell)$$

ℓ = last step

Modular Arithmetic

Recall, the set of all integers congruent to "a modulo m" is the congruence class:

$$[a]_{\text{mod } m} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

congruence class of a modulo m

e.g., $[2]_{\text{mod } 5} = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$

$[0]_{\text{mod } 5} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$

$\mathbb{Z}_n$ denotes "the integers mod n":

$\{0, 1, \ldots n-1\}$

Theorem If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

This shows that additions and multiplications preserve congruences.

Proof Let $a \equiv b$ and $c \equiv d \pmod{m}$.

Then $b = mq + a$ and $d = mk + c$

$$b + d = (mq + a) + (mk + c) = m(q + k) + (a + c)$$

Let $q+k = L$

$$\overbrace{b+d} = mL + \overbrace{(a+c)}$$

By def'n

$$b+d \equiv a+c \pmod{m}$$

Explaining how we got from the second-last line to the last line, as was asked during class.

$$a \equiv b \pmod{n}$$

$\downarrow$ By def'n this means

$$a = nq + b$$

This is equivalent to Definition 4 from week1-2.pdf (if the difference between a and b is divisible by n, then a and b are congruent in mod n)

Now,

$$bd = (mq+a)(mk+c)$$

$$= mqmk + mqc + amk + ac$$

$$= m\underbrace{(qmk + qc + ak)}_{S} + ac$$

$$bd = mS + ac \xrightarrow{\text{By def'n}} bd \equiv ac \pmod{m}$$

Inverses

$\oplus, \otimes, \ominus, \oslash$ to represent $+, \times, -, /$ in mod n.

$$x + 1 \equiv 3 \pmod 5$$

$$x \equiv 3 + (-1) \pmod 5$$

$$\equiv 3 + 4 \pmod 5$$

$$\equiv 7 \pmod 5$$

$$\equiv 2 \pmod 5$$

After class, several students asked me why we turned -1 into 4. This was done for two reasons:

1) To show that -1 can be replaced with any integer that it is congruent to in Z_5. In other words, you can add (or subtract) any multiple of 5 and the result will be the same.

2) We are working in Z_5, i.e., the set {0, 1, 2, 3, 4}. So any other integer can be mapped to an integer from within that finite set.