Tomorrow – 12:00
University 210
Galois connections

Goal: give an (efficient) algorithm for computing gcds. (writing $(a,b) = ma + nb$ too!)

Note: we have an algorithm for computing gcds!
1. Factor a and b ⟵ inefficient!
2. Compare prime factors / multiply all common prime factors

Ex: $(36, 122)$

$$36 = 2^2\, 3^2$$
$$122 = 2 \cdot 61$$
$$\longrightarrow (36, 122) = 2$$

$122 = 3 \cdot 36 + 14$	$(122, 36) = (86, 36) = (50, 36)$ $= (14, 36)$
$36 = 2 \cdot 14 + 8$	$(14, 36) = (14, 22) = (14, 8)$
$14 = 1\, 8 + 6$	$(14, 8) = (6, 8)$
$8 = 1 \cdot 6 + 2$	$(6, 8) = (6, 2)$

$6 = 3 \cdot 2$

$(6,2) = (4,2) = (2,2) = (0,2)$
$= 2$

Lesson: Remainders are key!

More formally...

Suppose $a \geq b > 0$

$a = r_0$, $b = r_1$

$0 \leq r_2 < b$

$a = bq_1 + r_2$

$0 \leq r_3 < r_2$

$b = r_2 q_2 + r_3$

$r_2 = r_3 q_3 + r_4$

$\vdots$

$r_{n-2} = r_{n-1} q_{n-1} + r_n$

$r_{n-1} = r_n q_n + 0$

$(a, b) = (r_2, b)$

$(r_2, b) = (r_2, r_3)$

Thm: Using ↑ notation, $(a,b) = r_n$
(the last nonzero remainder)

Q: ① Why is $r_n = (a, b)$?

② Why does the algorithm finish?

A2: $b > r_2 > r_3 > r_4 > \dots \geq 0$

If, $r_2, r_3, r_4 \dots$ were an infinite sequence of nonzero integers, there would be inf. many distinct integers b/n 0 and b. (not the case!)

So some $r_n = 0$

A1: $(a, b) = (a - bq_1, b) = (r_2, b)$

$= (r_2, b - r_2 q_2) = (r_2, r_3)$

$= (r_2 - r_3 q_3, r_3) = (r_4, r_3)$

$= \dots = (r_{n-1}, r_n)$

$= (r_{n-1} - r_n q_n, r_n) = (0, r_n) = r_n$

Ex: Compute $(105, 44)$

$$105 = 44 \cdot 2 + 17$$
$$44 = 17 \cdot 2 + 10$$
$$17 = 10 \cdot 1 + 7$$
$$10 = 7 \cdot 1 + 3$$
$$7 = 3 \cdot 2 + \boxed{1}$$
$$3 = 3 \cdot 1 + 0$$

$(105, 44) = 1$

Ex: Compute (F_{n+1}, F_{n+2}) where F_n is the n^{th} term in the Fibonacci sequence

Q: F_{n+2} divided by F_{n+1}?

$n = n+2-3+1$ equs.

$$\left\{\begin{aligned} F_{n+2} &= F_{n+1} + F_n \\ F_{n+1} &= F_n + F_{n-1} \\ &\ \vdots \\ F_4 &= F_3 + F_2 \\ F_3 &= F_2 \cdot 2 + 0 \end{aligned}\right.$$

(note: $0 \le F_n < F_{n+1}$)

$F_0 = 0$	
$F_1 = 1$	
$F_2 = 1$	
$F_3 = 2$	
$F_4 = 3$	

$$(F_{n+2}, F_{n+1}) = F_2 = 1$$

Linear Combinations

$$105 = 44 \cdot 2 + 17$$
$$44 = 17 \cdot 2 + 10$$
$$17 = 10 \cdot 1 + 7$$
$$10 = 7 \cdot 1 + 3$$
$$7 = 3 \cdot 2 + 1 \quad \text{start}$$
$$3 = 3 \cdot 1 + 0$$

Goal: write 1 as lin. comb. of 105, 44

$$1 = 7 - 3 \cdot 2$$
$$= 7 - (10 - 7 \cdot 1) \cdot 2$$
$$= 7 \cdot 3 - 10 \cdot 2$$
$$= (17 - 10) \cdot 3 - 10 \cdot 2$$
$$= 17 \cdot 3 - 5\ 10$$
$$= 17 \cdot 3 - 5\ (44 - 17 \cdot 2)$$
$$= 17 \cdot 13 - 5 \cdot 44$$
$$= (105 - 44 \cdot 2)\ 13 - 5 \cdot 44$$
$$= 105 \cdot 13 - 31 \cdot 44$$

Extended Euclidean algorithm:

Let $a, b \in \mathbb{Z}$ with $a \geq b \geq 1$.

Then $(a, b) = s_n a + t_n b$ where

$$s_0 = 1 \qquad t_0 = 0$$
$$s_1 = 0 \qquad t_1 = 1$$
$$s_j = s_{j-2} - q_{j-1} s_{j-1} \qquad t_j = t_{j-2} - q_{j-1} t_{j-1}$$

Pf: We will show $r_j = s_j a + t_j b$

If we do this, $(a,b) = r_n = s_n a + t_n b$

To show this, use strong induction

Note $r_0 = a = 1 \cdot a + 0 \cdot b$

$= s_0 a + t_0 b$ ✓

$r_1 = b = 0 \cdot a + 1 b$

$= s_1 a + t_1 b$ ✓

Suppose $\underline{r_j = s_j a + t_j b \text{ for all } j < k}$

Goal: show $r_k = s_k a + t_k b$

By Euclidean algorithm

$r_k = r_{k-2} - r_{k-1} q_{k-1}$

induction hyp: $r_{k-2} = s_{k-2} a + t_{k-2} b$

$\overset{\downarrow}{=} (s_{k-2} a + t_{k-2} b) - (s_{k-1} a + t_{k-1} b) q_{k-1}$

$= a(s_{k-2} - s_{k-1} q_{k-1}) + b(t_{k-2} - t_{k-1} q_{k-1})$

$= a s_k + b t_k$

Ex: Write $(102, 222)$ as a lin. comb. of 102 and 222

$s_j = s_{j-2} - q_{j-1} s_{j-1}$

$s_0 = 1 \qquad t_0 = 0$

$s_1 = 0 \qquad t_1 = 1$

$222 = 2 \cdot 102 + 18 \qquad s_2 = 1 - 2 \cdot 0 \qquad t_2 = 0 - 2 \cdot 1$

$102 = 5 \cdot 18 + 12 \qquad s_3 = 0 - 5 \cdot 1 \qquad t_3 = 1 - 5 \cdot (-2)$

$18 = 1 \cdot 12 + 6 \qquad s_4 = 1 - 1 \cdot (-5) \qquad t_4 = -2 - 1 \cdot 11$

$12 = 2 \cdot 6 + 0$

$s_4 a + t_4 b$

$6 \cdot 222 + (-13) \cdot 102 = 6 = (222, 102)$