A Modular GCD Algorithm

By Anna, Bernhard and David

Outline

- Basics
- Modular GCD of Integers
- Modular GCD of Polynomials

Basics in GCD Computations

- GCD g of non zero elements

1. g divides $a_1, ..., a_n$ and
2. every divisor of $a_1, ..., a_n$ divides g.

- Euclid's algorithm

$$a_i = a_{i-2} - q_i \cdot a_{i-1}, \text{ for } i = 3, ..., k$$

- Bèzout cofactors

$$gcd(a_1, a_2) = s \cdot a_1 + t \cdot a_2$$

$$s = a_1^{-1} \bmod a_2 \text{ and } t = a_2^{-1} \bmod a_1.$$

Modular GCD

- ϕ_p is homomorphism function

$$\begin{tikzcd} \text{gcd in Z} & Z \times Z \arrow[r, "\phi_p"] \arrow[d] & Z_p \times Z_p \arrow[d] & \text{gcd in } Z_p \\ & Z \arrow[r, "\phi_p"] & Z_p & \end{tikzcd}$$

- Steps:
  - Select primes
    - Unlucky primes
      - computed result is not the gcd
      - example: $a(x) = x - 3$, $b(x) = x + 2$, $\gcd(a, b) = 1$, mod 5 : $\gcd(a, b) = x + 2$
  - Convert a and b to modular representation
  - Reduction loop
  - Return result in standard representation

Large growing coefficients

Problem:
Coefficients are growing to large number while computing the GCD

Solutions:

- monic after each reduction, but needs extra GCD computations
- or...

$$r_0 := 824x^5 - 65x^4 - 814x^3 - 741x^2 - 979x - 764$$

$$r1 := 216x^4 + 663x^3 + 880x^2 + 916x + 617$$

$$q1 := \frac{103}{27}x - \frac{5837}{486}$$

$$r2 := \frac{614269}{162}x^3 + \frac{539085}{243}x^2 + \frac{1863490}{243}x + \frac{3230125}{486}$$

$$q2 := \frac{34992}{614269}x + \frac{30072401334}{377326404361}$$

$$r3 := -\frac{23256341085690}{377326404361}x^2 - \frac{27844657381944}{77326404361}x + \frac{32938754949612}{377326404361}$$

$$q3 := -\frac{2317799130804271 09}{3767527255881780}x - \frac{21250438136739791430061 2023767}{73015749093683618269574773 50}$$

$$r4 := \frac{16363047386796678464177 1618997}{150238166859431313311882 25}x + \frac{27604692189910198127667 2067323}{300476333718862626623764 50}$$

$$q4 := -\frac{34939900525717422066436421955424400 0250}{61742098348486478706658122441075651245917}x - \frac{53605502942609915156276524064879156029311616760832823425}{26774931978255360791810790390285343980469602246030531286009}$$

$$r5 := \frac{14999180998204546086628509444183593910034968673275}{1419192066539766667946619608091293820743154 18338}$$

$$q5 := 23222307035756106796937177832200054614723837798596144162324081189217602966 98/22534494575630661208071063858852539249064234560986748981846048685755 2186875x + 1958818007759640557915662822891805286108190368068267555474109561947740223845 87/22534494575630661208071063858852539249064234560986748981846048685755 2186875$$

Motivation

Modular GCD computation with...

- ... Polynomials:
  - eliminated risk of large growing coefficients
- ... Integers:
  - more efficient and much faster than the original representation
  - arithmetic operations can be performed on parallel processors