Algorithms in Algebra and Number Theory

(0)

Fabian Gundlach
gundlach@math.harvard.edu fabiangundlach.org/21-fall/2[redacted]

OH: Tentatively TuTh 2-3pm room 233

References:
- A course in computational Algebraic Number Theory, Cohen (1993) Pari
- Algorithmic Algebraic Number Theory, Pohst-Zassenhaus (1989) [later topics...]
- The Art of Computer Programming, [redacted] Vol. 1 (Fundamental Algorithms) + Vol. 2 (Seminumerical Algorithms), Knuth (1973+1981) [earlier topics]

Implementation exercises:
projecteuler.net

HW ungraded

Final paper

some important algorithms – how not to ...

1) ... add integers? [Joke...]

Stupid schoolbook addition:

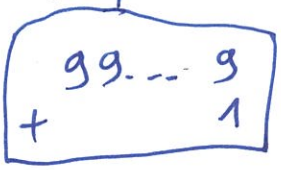
$$
\begin{array}{r}
1\,\tfrac{1}{6}\,3\,4\,5\,8\,2\,5 \\
+\;\tfrac{1}{2}\,6\,5\,9\,0\,7\,6 \\
\hline
=\;1\,8\,9\,9\,4\,8\,9\,1 \\
+\;\;\;\;\;\;1\,0\,0\,1\,0 \\
\hline
=\;1\,8\,9\,0\,4\,8\,0\,1 \\
+\;\;\;\;\;1\,0\,0\,1\,0\,0 \\
\hline
=\;1\,8\,0\,0\,4\,9\,0\,1 \\
+\;\;1\,0\,0\,0\,0\,0\,0 \\
\hline
=\;1\,9\,0\,0\,0\,4\,9\,0\,1
\end{array}
$$

} n digits

[redacted]

Worst case: $\Omega(n^{\bullet})$ [redacted] lines,

$\Omega(n^2)$ digits



~~Now not to~~

2) ... multiply polynomials $f, g \in \mathbb{F}_p[X]$

(= [illegible] given the coeffs. of f, g, determine the coeffs of fg):

Schoolbook mult:

$$f = \sum_{i=0}^{n} a_i X^i, \quad g = \sum_{j=0}^{m} b_j X^j$$

$$\rightsquigarrow fg = \sum a_i b_j X^{i+j} = \sum_{k=0}^{n+m} c_k X^k$$

with $c_k = \sum_{\substack{i \le n, \\ j \le m: \\ i+j=k}} a_i b_j$.

The total number of summands in $c_0, \dots, c_{n+m}$ is $n \cdot m$.

But we can actually compute $c_0, \dots, c_{n+m}$ in "roughly linear" time [illegible]

$O_{p,\varepsilon}((n+m)^{1+\varepsilon})$.

3) ... divide polynomials $f, g \in \mathbb{F}_p[X]$.

(given the coeffs. of f, g, determine the coeffs. of $q, r \in \mathbb{F}_p[X]$ with $f = gq + r$, $\deg(r) < \deg(g)$):

"$r = f \bmod g$"

Schoolbook division:

Let $n = \deg(f)$, $m = \deg(g)$

$h_n := f$

For $i = n, \dots, m$, let

$$c_i := \frac{X^i\text{-coeff. of } h_i}{\underbrace{\text{leading coeff. of } g}_{X^m\text{-}}},$$

$$h_{i-1} := h_i - c_i X^{i-m} \cdot g.$$

$\deg(h_n) = n \Rightarrow \deg(h_{n-1}) \leq n-1 \Rightarrow \deg(h_{n-2}) \leq n-2$

$\Rightarrow \dots \Rightarrow \deg(h_{m-1}) \leq m-1$

$$f = \underbrace{\left(\sum_{i=m}^{n} c_i X^{i-m}\right)}_{\text{quotient } q} \cdot g + \underbrace{h_{m-1}}_{\text{remainder}}$$

~~In the worst case,~~ we

$\rightsquigarrow$ running time $\Theta_p((n-m)m)$.

But can be done in $\mathcal{O}_p((n+m)^{1+\varepsilon})$.

4 (b) ... find the gcd of polynomials $f, g \in \mathbb{F}_p[X]$:

Euclidean algorithm:

$a_0 := f$

$a_1 := g$

$a_2 := a_0 \bmod a_1$

$a_3 := a_1 \bmod a_2$

$\vdots$

$a_{i+2} := a_i \bmod a_{i+1}$

$\vdots$

$a_k = \ldots \neq 0$

$a_{k+1} = 0$

$\gcd(f,g) = a_k$

Thm There are pol. f, g of degrees $n, n-1$ such that

$\deg(a_i) = n-i \quad , \quad k = n.$

$(\text{So } \sum \deg(a_i) = \Theta(n^2).)$

Pf Work backwards:

$a_n := 1, \quad a_{n-1} := X,$

$a_i := a_{i+2} + X^{\square} \cdot a_{i+1}$ for $i = n-2, \ldots, 0.$

$f := a_0, \quad g := a_1.$ □

But $\gcd(f,g)$ can be computed in $O_p((n+m)^{\varepsilon})$.

5) -- find $\gcd(f,g)$ for $f,g \in \mathbb{Q}[x]$:

W.l.o.g. $f,g \in \mathbb{Z}[x]$, $\deg(f) \geq \deg(g)$.

Euclidean algorithm:

$a_0 := f$

$a_1 := g$

$a_{i+1} := \text{lc}(a_i)^{\deg(a_i)-\deg(a_{i+1})+1} \cdot a_i \bmod a_{i+1}) \in \mathbb{Z}[x]$

$\vdots$

until

$a_{k+1} = 0$.

$\Rightarrow \gcd(f,g) = a_k$.

relatively prime

Thm For any (large) $n \in \mathbb{Z}$, there are pol. $f,g \in \mathbb{Z}[x]$ of degrees $n, n-1$ such that each coeff. of f,g has $\mathcal{O}(n)$ digits, $k=n$, and $a_n \in \mathbb{Z}$ has $\Omega((1+\sqrt{2})^n)$ digits.

Pf Let $b_n = 1$, $b_{n-1} = x$,

$b_i = b_{i+1} + x^{\cdot} \cdot b_{i+1}$ for $i = n-2, \dots, 0$.

$\Rightarrow \deg(b_{n-i}) = i$,

$\text{lc}(b_{n-i}) = 1$

$b_{i+1} = (b_{i-1} \bmod b_i)$

(max. coeff. of b_i) $\leq$ (max. coeff. of b_{i+1}) + (max. coeff. of

$\Rightarrow$ (max. coeff. of b_{n-i}) $\leq F_i = \mathcal{O}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{b_{i+2}}\right)$

i-th Fibonacci nr.

$\Rightarrow$ Each coeff. of $b_0, b_1 \in \mathbb{Z}(x)$ has $\mathcal{O}(n)$ digits.

Let $f = b_0$, $g = 2 \cdot b_1$.

$\quad\; \| \qquad\quad \|$

$\quad a_0 \qquad\quad a_1$

~~By induction, $a_i =$~~

~~If $a_i = 2^{r_i} \cdot b_i$~~

Claim: ~~By induction,~~ $a_i = 2^{r_i} \cdot b_i$, where

$r_0 = 0$, $r_1 = 1$, $r_{i+2} = 2 r_{i+1} + r_i$:

Pf by ind: $\{ a_{i+2} = \Big(\underbrace{lc(a_{i+1})}_{2^{r_{i+1}}}^{\overbrace{\deg(a_i) - \deg(a_{i+1}) + 1}^{2}} \cdot \underbrace{a_i}_{2^{r_i} \cdot b_i} \bmod \underbrace{a_{i+1}}_{2^{r_{i+1}} b_{i+1}} \Big)$

$= \left(2^{2 r_{i+1} + r_i} \cdot b_i \bmod b_{i+1} \right)$

$= 2^{2 r_{i+1} + r_i} \cdot b_{i+2} \}$ □

We have

$r_i = \Theta\left((1+\sqrt{2})^i \right)$, so in particular

$a_n = 2^{r_n}$ has $\Theta\left((1+\sqrt{2})^n \right)$ digits. □

~~$x^2 - 2x - 1 = 0$~~

~~$\frac{2 \pm \sqrt{4+4}}{2} = 1 \pm \sqrt{2}$~~

```
a_0 = 3 * X^10 + 5 * X^9 + 4 * X^8 + 5 * X^7 + 3 * X^6 + 3 * X^5 + 2 * X^4 + 2 * X^3 + 4 * X^2
+ 1 * X^1 + 5 * X^0

a_1 = 2 * X^9 + 1 * X^8 + 2 * X^7 + 2 * X^6 + 1 * X^5 + 2 * X^4 + 2 * X^3 + 2 * X^2 + 2 * X^1
+ 2 * X^0

a_2 = - 3 * X^8 - 6 * X^7 - 8 * X^6 - 7 * X^5 - 18 * X^4 - 18 * X^3 - 10 * X^2 - 22 * X^1 + 6
* X^0

a_3 = 24 * X^7 + 48 * X^6 - 36 * X^5 + 72 * X^4 + 120 * X^3 - 24 * X^2 + 252 * X^1 - 36 * X^0

a_4 = - 7200 * X^6 + 1152 * X^5 - 1728 * X^4 - 12096 * X^3 + 12384 * X^2 - 15264 * X^1 + 3456
* X^0

a_5 = - 1734856704 * X^5 + 997318656 * X^4 + 3845947392 * X^3 + 740524032 * X^2 + 7963619328 *
X^1 - 576294912 * X^0

a_6 = - 584086607484891955200000 * X^4 - 655857649653173452800000 * X^3 -
660383462240708198400000 * X^2 - 800105889145238323200000 * X^1 + 1338805978908327936000 * X^0

a_7 = 85294557988032224162323393075009959128274567168000000000 * X^3 -
7269613138948848401510110203640997250682847232000000000 * X^2 +
120472993055746469176227837908857009978428358656000000000 * X^1 +
3371294386566795915983946654443400064942473216000000000 * X^0

a_8 =
759959439005460743286470953594226985289840623006408436416906146168200753258283944841444538766
958631077726388224000000000000000000000 * X^2 +
1597984990559247565932903117430723401512089792652232663589046921980206485675730428013523181085
9666649474784034816000000000000000000000 * X^1 +
117691166288399132936576597713504462745927005670406337985862155961888258805595635817815251965 2
0113785028112023552000000000000000000000 * X^0

a_9 =
219922562057631600790062251868805972311930573543585982692183670398783601461410405968151775385 6
338182990328044155118056126947770502982179703590541859421531902935876623951316246418105182758 5
697214456802672884593814903256221871928447975366309267338668382913786461737910796288000000000 0
000000000000000000000000000000000000000 * X^1 +
168861412149565397862256227823371127490589712111783187118000886880503963016277779729203053995 5
239367161138798949039436118312838039004753607159610316125096914764356096600386908672426312501 6
357583689089616108104525030157826194001600639927479202029452549958007407315861372928000000000 0
000000000000000000000000000000000000000 * X^0

a_10 =
192485838137508555438088464927810337773853062688045902913590832351722138715573218705267956858 8
760493643938360031748731193153913665301319070831224843720854191402284242435364018047720386066 2
937206786303927550190101395618703425663414764681263486475658655756812308387362455465113546446 5
537468407338960266461000970753673274462548297829030710865252184839402549807060240070769020764 4
141889270791752341711361831580111951253327461944855115331099776635449595227923333006681154309 7
318866100378310738957826043683716851278004076045368243745248870087707046817854243486522334344 1
183467215160873651831370697132893806985857256120228637078099587090040445649565244287090688000 0
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 0
0000000000000000000 * X^0
```

6) ... find the roots in $\mathbb{F}_p$ of a pol. $f(x) \in \mathbb{F}_p[x]$ of degree n:

For each $x \in \mathbb{F}_p$, check whether $f(x) = 0$.

Time $\mathcal{O}(p\,n)$ even if you could do arithmetic in $\mathbb{F}_p$ in $\mathcal{O}(1)$.

can be done $\mathcal{O}((\log p)^{\cdots} \cdot n \cdot (\log n)^{\cdots})$

with a nondeterministic alg. in expected time

7) ... find the number of primes $p \le n$:

Use the sieve of Eratosthenes

Running time $\mathcal{O}\left(\sum_{p \le n} \frac{n}{p}\right) = \mathcal{O}(n \log\log n)$

Some problems that have no "obvious" algorithm at all:

8) Factor pol. in $\mathbb{Q}[X]$.

9) Find the ring of integers, class group, unit group of a number field $K = \mathbb{Q}[X]/f(X)$.

10) Find the Galois closure of a field ext. $L|K$ and the Galois group.

11) Find the dimension, number of irred. comp., ... of a variety $\{P \in K^n \mid f_1(P) = \ldots = f_m(P) = 0\}$.

Some problems are undecidable:

12) Does a given pol. $f \in \mathbb{Z}[x_1, \ldots, x_n]$ have a root $(x_1, \ldots, x_n) \in \mathbb{Z}^n$?