Rmk 14.7 van Hoeij (Factoring polynomials and the knapsack problem) found another alg. that seems to work better in practice (but without rigorous analysis of the running time): Idea:

For simplicity, assume $lc(f)=1$.

How can we tell whether the pol. g in Rmk 14.5 has short length ($< ~~\ldots~~ A$)?

For a pol. f of degree n with roots $\alpha_1, \ldots, \alpha_n$, let

$$Tr^i(f) := \alpha_1^i + \ldots + \alpha_n^i \qquad (i = 0, 1, \ldots).$$

~~\ldots~~ Note that the coeff. of f are ~~\ldots~~ the el. symm. pol. in $\alpha_1, \ldots, \alpha_n$, which can be written as pol. in $Tr^i(f)$ ~~\ldots~~ $(i = 1, \ldots, n)$. Conversely, we can write $Tr^i(f)$ as pol. in the coeff. of f.

Hence, $|f|$ small $\Leftrightarrow$ $\left|\underbrace{\begin{pmatrix} Tr^1(f) \\ \vdots \\ Tr^n(f) \end{pmatrix}}_{Tr(f)}\right|$ small.

Clearly, $Tr(fg) = Tr(f) + Tr(g)$.

~~\ldots~~

Finding ~~\ldots~~ a short $g \equiv \prod_{i \in S} a_i \mod p$ corresponds to finding $e_1, \ldots, e_n \in \{0, 1\}$ $\quad (e_i = 1 \Leftrightarrow i \in S)$

such that there is a short vector

$$v = \sum_{i \in S} Tr(a_i) + pw = \underbrace{\sum_i e_i Tr(a_i) + pw}_{} \quad \text{with } w \in \mathbb{Z}^n.$$

If we allowed arbitrary $e_i \in \mathbb{Z}$, these would form a lattice.

Rmk Say you know a complex number $r \in \mathbb{R}$ which is approximate an algebraic number. How to find the min. pol. $f \in \mathbb{Z}[X]$?

Say $|f| \leq A$, $|f(r)| \leq B$, $\deg(f) \leq n$.

Look for a short vector (length $\in O(1)$) in the rank $n+1$ lattice

$$\Lambda = \left\{ \left(\underbrace{\frac{f}{A}}_{\in \mathbb{R}^{n+1}}, \underbrace{\frac{f(r)}{B}}_{\in \mathbb{C} \cong \mathbb{R}^2} \right) \;\middle|\; f \in \mathbb{Z}[X] \text{ of deg.} \leq n \right\} \subseteq \mathbb{R}^{n+3}.$$

Rmk You could also use this for a nonrigorous factoring alg.:
Find a complex root r of f and then find its min. pol. g.

15. Primality testing and integer factorization

Rmk If $n = p_1^{e_1} \cdots p_k^{e_k}$, then

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_k^{e_k}$$

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{e_1})^\times \times \cdots \times (\mathbb{Z}/p_k^{e_k})^\times .$$

Rmk If p is an odd prime and $e \geq 1$, then $(\mathbb{Z}/p^e)^\times$ is isomorphic to the cyclic group $C_{\varphi(p^e)}$ of order $(p-1)p^{e-1} = \varphi(p^e)$.

$\rightsquigarrow (\mathbb{Z}/n\mathbb{Z})^\times \cong C_{(p_1-1)p_1^{e_1-1}} \times \cdots \times C_{(p_k-1)p_k^{e_k-1}}$ if n is odd.

~~Lemma Given $n \geq 2$, we can determine whether n is a perfect power ($n = m^k$ for some $m \in \mathbb{Z}$, $k \geq 2$) in $\tilde{O}((\log n)^?)$.~~

~~Pf For each $2 \leq k \leq \log_2(n)$, compute $\lfloor \sqrt[k]{n} \rfloor$ using Newton's method (in time $\tilde{O}(\log$~~

~~Hence, we can easily assume that n is odd and not a perfect power.~~

~~Rmk Unlike for pol in $\mathbb{F}_q[T]$, we have no pol time alg. for finding the squarefree factorization of $n \in \mathbb{Z}$, or even to determine whether n is squarefree~~

Rmk Let $n \geq 2$. Then, the set

$$S := \{ a \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a^{n-1} \equiv 1 \bmod n \}$$

forms a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.

In part., either

a) $S = (\mathbb{Z}/n\mathbb{Z})^\times$ or

b) $|S| \leq \frac{1}{2} \cdot |(\mathbb{Z}/n\mathbb{Z})^\times| = \frac{\varphi(n)}{2} < \frac{n}{2}$.

$\left(H \leq G \Rightarrow |H| = \frac{|G|}{[G:H]} \right)$

Def Integers $n \geq 2$ with $S = (\mathbb{Z}/n\mathbb{Z})^\times$ are called <u>Carmichael numbers</u>.

Rmk Any prime is a Carmichael number (little Fermat).

Lemma 15.1 An odd number $n = p_1^{e_1} \cdots p_k^{e_k}$ is a Carmichael number if and only if

$$\varphi(p_i^{e_i}) \mid n-1 \text{ for all } i.$$

Pf

"$\Leftarrow$"
$\varphi(p_i^{e_i}) \mid n-1$
$\Rightarrow a^{n-1} \equiv 1 \bmod p_i^{e_i} \quad \forall i$
$\Rightarrow a^{n-1} \equiv 1 \bmod n$

"$\Rightarrow$" Take any a s.t. a mod $p_i^{e_i}$ generates the cyclic group $(\mathbb{Z}/p_i^{e_i})^\times$ of order $\varphi(p_i^{e_i}) \not\equiv 0 \bmod n-1$. $\square$

Ex $n = 3 \cdot 11 \cdot 17$ is a Carmichael number.

Lemma 15.2 Every Carmichael number is squarefree.

Pf. If $e_i \geq 2$, then $p_i \mid \varphi(p_i^{e_i})$, but $p \nmid n-1$. $\square$

Thm 15.5 The following randomised Monte Carlo alg. detects whether an odd number $n \geq 3$ is Carmichael with a false pos. ~~prob~~. $\leq \frac{1}{2}$ and no false negatives and average running time $\tilde{O}((\log n)^2)$.

Alg

Pick $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ uniformly at random.

Answer Carmichael if $a^{n-1} \equiv 1 \bmod n$. $\square$

Lemma 15.3 We can pick $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ uniformly at random in expected time $\tilde{O}(\xi \log n)$.

Alg Pick $a \in \mathbb{Z}/n\mathbb{Z}$ uniformly at random. If $\gcd(a,n) \neq 1$, start over.

Pf The ~~running~~ expected running time is $\tilde{O}\left((\log n) \cdot \frac{n}{\varphi(n)}\right)$. $\square$

Lemma 15.4 We have $\frac{n}{\varphi(n)} \ll \log\log n$ for large n.

Pf $$\frac{n}{\varphi(n)} = \prod_{p \mid n} \frac{1}{1-\frac{1}{p}}$$

$$\Rightarrow \log \frac{n}{\varphi(n)} = \sum_{p \mid n} \log \frac{1}{1-\frac{1}{p}} = \sum_{p \mid n} \left(\frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \dots\right)$$

$$\leq \sum_{p \mid n} \frac{1}{p} + O(1)$$

If K is the largest number s.t. $\prod_{p \leq K} p \leq n$, then

$$\sum_{p \mid n} \frac{1}{p} \leq \sum_{p \leq K} \frac{1}{p} \sim \log\log K$$

with $K \leq \log n + O(1)$. $\square$