Distinct degree factorization (Gauss, Disqu. Arith., §370-1)

Fact: $$x^{q^i} - x = \prod_{\substack{f \text{ irreducible over } \mathbb{F}_q \\ \deg(f) \text{ divides } i}} f(x)$$

Write $$f^{[i]} = \prod_{\substack{g \text{ irred. factor of } f \\ \deg(g) = i}} g$$

$f^* \leftarrow f$; `/* squarefree */`

`for` $i \leftarrow 1, \ldots, \lfloor n/2 \rfloor$ `do`

`{`$f^{[i]}(x) \leftarrow \mathrm{GCD}(-x + x^{q^i} \bmod f^*(x), f^*(x))$;

$f^* \leftarrow f^* \big/ f^{[i]}$;

`}`

$f^{[\deg(f^*)]} \leftarrow f^*$; `/* factor with degree` $> \lfloor n/2 \rfloor$ `*/`

Suppose $f(x) \in \mathbb{F}_q[x]$ has degree n, $g(x)$, $h(x)$ are modular residues.
All counts are in terms of arithmetic operations in $\mathbb{F}_q$.

Problem	Complexity	Inventors of algorithm
1. $g \cdot h \pmod{f}$	$O(n(\log n) \operatorname{loglog} n)$	Schönhage & Strassen 1969 Schönhage 1977 ($p = 2$)
2. $\mathrm{GCD}(f, g)$	$O(n(\log n)^2 \operatorname{loglog} n)$	Knuth 1971/Moenck 1973
3. $g^q \pmod{f}$	$O((\log q) n^{1+o(1)})$	using Pingala 200 b.c.
4. $g(h(x)) \pmod{f(x)}$	$O(n^{1.67})$	using Brent & Kung 1978, Huang & Pan 1997
5. $x^{q^n} \pmod{f(x)}$ given $x^q \pmod{f(x)}$	$O(n^{1.67})$	von zur Gathen & Shoup 1991

6. $g(h_1), ..., g(h_n) \pmod{f}$ $O(n^{2+o(1)})$ using Moenck & Borodin 1972

7. $x^{q^2}, ..., x^{q^n} \pmod{f(x)}$ $O(n^{2+o(1)})$ von zur Gathen & Shoup 1991
given $x^q \pmod{f(x)}$

Fast computation of $x^{q^n} \bmod f(x)$

$$x^{q^i} \equiv (\underbrace{x^{q^{i-1}}}_{h_{i-1}(x)})^q$$

$$\equiv h_{i-1}(\underbrace{x^q}_{h_1(x)}) \qquad \Longleftarrow \qquad (a+b)^q = a^q + b^q \text{ in } \mathbb{F}_q$$

$$\equiv h_{i-1}(\, h_1(x)\,)$$

$$\equiv h_{\lfloor i/2 \rfloor}(\, h_{\lfloor i/2 \rfloor}(\, h_{i \bmod 2}(x)\,)\,) \pmod{f(x)}$$

(modular polynomial composition)

Fast modular polynomial composition

Compute $g(h(x)) \pmod{f(x)}$ with $O(n^{1.69})$ field operations.

$$g(x) = \sum_{j=0}^{\lceil\sqrt{n}\rceil} \left(\sum_{l=0}^{\lfloor\sqrt{n}\rfloor-1} c_{j,l} x^l \right) \cdot x^{\lfloor\sqrt{n}\rfloor \cdot j}$$

$$[c_{j,l}] \qquad \cdot \qquad \begin{bmatrix} \overrightarrow{h^0 \bmod f} \\ \overrightarrow{h^1 \bmod f} \\ \overrightarrow{h^2 \bmod f} \\ \vdots \\ \overrightarrow{h^{\lfloor\sqrt{n}\rfloor-1} \bmod f} \end{bmatrix}$$

$$\lfloor\sqrt{n}\rfloor \times \lfloor\sqrt{n}\rfloor \quad \lfloor\sqrt{n}\rfloor \times n \qquad \Rightarrow O(\sqrt{n}(\sqrt{n})^{2.38})$$

Equal degree factorization (Cantor & Zassenhaus 1981, Ben-Or 1981)

Fact: $$x^{q^i} - x = \prod_{a \in \mathbb{F}_q} \left(a + x + x^q + x^{q^2} + \cdots + x^{q^{i-1}}\right)$$

(trace of Frobenius autom. $\mathbb{F}_{q^i} \to \mathbb{F}_q$)

`/*` f `has irreducible distinct factors of degree` d`,` $q = p^k$ `*/`

Step 1 Pick a <u>random</u> α mod f;

$\beta \equiv \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{kd-1}}$ mod f; `/*` $\mathbb{F}_{q^d} \to \mathbb{F}_p$ `*/`

Step 2 If $p > 2$ then $\gamma \equiv \beta^{(p-1)/2}$ mod f else $\gamma = \beta$;

Step 3 Recursively factor $g_1 = \mathrm{GCD}(\gamma, f)$, $g_2 = \mathrm{GCD}(1 + \gamma, f)$, and $f/(g_1 g_2)$;

Computing $x^q \bmod f(x)$ with $f(x) \in \mathbb{F}_q[x]$ where $q = 2^n$ by squaring

(Pingala's method)

Suppose $\mathbb{F}_q = \mathbb{F}_2[z]/(\varphi(z))$, i.e., $f \in \mathbb{F}_2[x, z]$ and $\varphi \in \mathbb{F}_2[z]$:

$$\boxed{\begin{array}{l} h_0(x) \leftarrow x; \\ \texttt{for } i \leftarrow 1,\ldots,n \texttt{ do} \\ \quad \texttt{\{ } h_i \leftarrow h_{i-1}^2 \bmod (f,\varphi); \texttt{/* } h_i \equiv x^{2^i} \pmod{(f,\varphi)} \texttt{ */ \}} \end{array}}$$

Fixed-precision cost: $n \times \underbrace{n^{1+o(1)}}_{\text{polyn. arith. over } \mathbb{F}_q} \times \underbrace{n^{1+o(1)}}_{\text{arith. in } \mathbb{F}_q} = n^{3+o(1)}$

Computing $x^q \bmod f(x)$ with $f(x) \in \mathbb{F}_q[x]$ where $q = 2^n$ even faster

Suppose we already have

$$x^{2^i} \bmod f(x) = h_i(x) = c_0(z) + c_1(z)x + \cdots + c_{n-1}(z)x^{n-1} \in \mathbb{F}_q[x].$$

and

$$z^{2^i} \bmod \varphi(z) = \psi(z) \in \mathbb{F}_2[z].$$

Then

$$\begin{aligned}
x^{2^{2i}} &\equiv (c_0(z) + c_1(z)x + \cdots + c_{n-1}(z)x^{n-1})^{2^i} \pmod{(f(x), \varphi(z))} \\
&\equiv (c_0(z)^{2^i} + c_1(z)^{2^i} x^{2^i} + \cdots + c_{n-1}(z)^{2^i}(x^{n-1})^{2^i} \\
&\equiv (c_0(z^{2^i}) + c_1(z^{2^i})x^{2^i} + \cdots + c_{n-1}(z^{2^i})(x^{2^i})^{n-1} \\
&\equiv c_0(\psi) + c_1(\psi)h_i(x) + \cdots + c_{n-1}(\psi)h_i(x)^{n-1}
\end{aligned}$$

which can be computed with n modular polynomial compositions over $\mathbb{F}_2$—binary cost: $O(n \cdot n^{1.67})$,
and then one over $\mathbb{F}_q$—binary cost: $O(n^{1.67} \cdot n^{1+o(1)})$.

Computing the trace of the Frobenius automorphism

We want

$$v(x) + v(x)^p + v(x)^{p^2} + \cdots + v(x)^{p^{kd-1}} \mod f(x)$$

and we have

$$h_{2^j}(x) \equiv x^{p^{2^j}} \pmod{f(x)} \quad j = 1, 2, \ldots, \lceil \log(kd) \rceil$$

Trick:

$$(\underbrace{v(x)^p + v(x)^{p^2} + \cdots + v(x)^{p^i}}_{w_i(x)})^{p^i} \equiv \begin{cases} w_i(x)^{p^i} \equiv \widetilde{w}_i(h_i) \\ v(x)^{p^{i+1}} + \cdots + v(x)^{p^{2i}} \equiv w_{2i}(x) - w_i(x) \end{cases}$$

hence one finds the entire trace of Frobenius in $O(n^{2.67})$ fixed-precision operations (given h_1).

Irreducibility testing is even faster

Theorem *Let* $\mathbb{F}_q = \mathbb{F}_2[z]/(\varphi(z))$ *with* $\deg(\varphi) = n$. *Then one can test if a polynomial of degree* n *over* $\mathbb{F}_q$ *is irreducible, or if all its irreducible factors are of equal degree and if so determine their common degree, with*

$$O(n^{2.67})$$

fixed precision deterministic operations.