IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

Joachim von zur Gathen

Technical Report No. 188/86

February 1986

Department of Computer Science
University of Toronto
Toronto, Ontario, Canada M5S 1A4

IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

Joachim von zur Gathen
University of Toronto

February 1986

Abstract.

Several methods of computing irreducible polynomials over finite fields are presented. If preprocessing, depending only on p, is allowed for free, then an irreducible polynomial of degree at least n over $\mathbf{Z}_p$ can be computed deterministically with $O(n \log p)$, i.e. O(output size), bit operations. The estimates for the preprocessing time depend on unproven conjectures.

Part of this work was done while the author was visiting Universität Zürich in 1984/85, and supported by Schweizerischer Nationalfonds, grant 2175-0.83, and by NSERC, grant 3-650-126-40.

Author's address: Department of Computer Science, University of Toronto, Toronto, Canada M5S 1A4

1. Introduction

The purpose of this paper is to give some deterministic methods for computing irreducible polynomials over finite fields. Such polynomials provide the field extensions required in several algorithms, such as factoring multivariate polynomials (Chistov & Grigoryev [1982], von zur Gathen [1985a], von zur Gathen & Kaltofen [1985a, 1985b], Lenstra [1985]) and very fast parallel arithmetic of polynomials (Eberly [1984]). The probabilistic polynomial-time methods available for problems such as factoring polynomials (Berlekamp [1967, 1970]) and generating irreducible polynomials (Rabin [1980]) are quite satisfactory in practice. However, it remains a theoretical challenge to find deterministic polynomial-time algorithms for these problems: see Camion [1983] for constructing large irreducible polynomials from small ones, von zur Gathen [1985b] for univariate factoring when $p-1$ is smooth (assuming ERH), and Kaltofen [1985] for multivariate irreducibility testing.

In Section 2 we collect the basic facts showing that certain (integral) cyclotomic polynomials are either irreducible modulo p, or at least have only large irreducible factors. These properties depend on certain conditions that have to hold between the characteristic p and another prime number q.

In Sections 3 and 4 we investigate these conditions, show some relations with classical problems in number theory (Fermat's conjecture and Artin's conjecture), and state reasonable but unproven conjectures saying that for every p there exists a small q satisfying the conditions. Numerical evidence supports these conjectures, and we prove that the conjectures hold for random primes.

Section 5 applies these conjectures to yield three fast algorithms for constructing irreducible polynomials over $\mathbf{Z}_p$. The most interesting is a deterministic method which, after a preprocessing stage involving p only, produces irreducible polynomials of degree at least n in time (= number of bit operations) proportional to the output size $O(n \log p)$ (in fact, in. $O(\log n)$ operations if we do not insist on the dense representation of polynomials). The conjectures (plus ERH) imply that the preprocessing stage can be performed deterministically in $(n \log p)^{O(1)}$ bit operations.

The unproven conjectures only concern the timing of the algorithm, not the correctness of the output. Furthermore, they only intervene in the preprocessing stage depending on p, but not on n.

The irreducible polynomials that we consider in this paper are very easy to compute, in linear time. After learning of the present results, Adleman & Lenstra [1986] proposed different methods for computing irreducible polynomials; their approach avoids the above conjectures, but seems to require more unwieldy (but still polynomial-time) computations in number fields.

2. Cyclotomic polynomials over finite fields

In this section we collect some well-known facts concerning prime numbers p and q which guarantee that for any $k \geq 1$ the q^k-th cyclotomic polynomial is either irreducible in $GF(p^e)[x]$, or that at least each irreducible factor is large. ($GF(p^e)$ is a field with p^e elements.)

If $a, m \in \mathbf{Z}$ with $m \geq 2$ and $\gcd(a, m) = 1$, then the order $s = \mathrm{ord}_m(a)$ of a modulo m is the smallest integer $t \geq 1$ such that $a^t \equiv 1 \bmod m$. Then s is a divisor of $\phi(m)$, where ϕ is the Euler function, and $a^{\phi(m)} \equiv 1 \bmod m$. a is called primitive modulo m if and only if $s = \phi(m)$. We write $q^i \,\|\, a$ if and only if q divides a exactly i times, i.e. if $i \geq 0$, $q^i \mid a$, and $q^{i+1} \nmid a$. We also write $a \dot{-} b = \max\{0, a-b\}$, and $a \dot{-} b \dot{-} c = (a \dot{-} b) \dot{-} c$.

Fact 2.1. Let $a, e, i, j, k, q, s \in \mathbf{Z}$ with q prime, $e, i, k \geq 1$, $j \geq 0$, $a \not\equiv 0 \bmod q$, $s = \mathrm{ord}_q(a)$, $q^i \,\|\, a^q - a$, and $q^j \,\|\, e$.

(i) If $q \geq 3$, then $\mathrm{ord}_{q^k}(a^e) = sq^{k \dot{-} i \dot{-} j} / \gcd(e, s)$.

(ii) If $q \geq 3$ and $k \geq 2$, then the following three properties are equivalent:

(2.1) a is primitive modulo q^k,

(2.2) a is primitive modulo q^2,

(2.3) a is primitive modulo q, and $a^q \not\equiv a \bmod q^2$.

(iii) If $q = 2$, $k \geq 3$, and a is congruent to 3 or 5 modulo 8, then $s = 1$ and $\mathrm{ord}_{2^k}(a^e) = 2^{k \dot{-} j \dot{-} 2}$.

For proofs of these facts, see e.g. Knuth [1981], 3.2.1.2, Theorem C, and Hasse [1980], Part 1, ch.4.

Throughout the paper, p and q denote prime numbers. For $m \in \mathbf{N}$, $\psi_m \in \mathbf{Z}[x]$ is the m-th cyclotomic polynomial. For properties of ψ_m, see e.g. Borevich & Shafarevich [1966]. ψ_m is irreducible and has degree $\phi(m)$. If F is a field, then $\Psi_{m,F} \in F[x]$ denotes the image of ψ_m given by the canonical mapping $\mathbf{Z} \rightarrow F$. The cyclotomic polynomials ψ_{q^k} are easy to describe:

Fact 2.2 (Lidl & Niederreiter [1983], Example 2.46). Let q be a prime, $k \geq i \geq 1$. Then

$$\psi_q = x^{q-1} + x^{q-2} + \cdots + 1 \in \mathbf{Z}[x],$$
$$\psi_{q^k} = \psi_{q^i}(x^{q^{k-i}}).$$

Fact 2.3 (Lidl & Niederreiter [1983], Theorem 2.47). Let p, q be distinct prime numbers, $e, k \geq 1$ (and $k \geq 3$ if $q = 2$), and $F = GF(p^e)$. Then each irreducible factor of $\Psi_{q^k, F}$ has degree $\mathrm{ord}_{q^k}(p^e)$.

Corollary 2.4. Let p, q, e, k, F be as in Fact 2.3, q odd, $s = \mathrm{ord}_q(p)$, and let $i \geq 1$ and $j \geq 0$ with $q^i \parallel p^q - p$ and $q^j \parallel e$. Suppose that $g \in F[x]$ is an irreducible factor of $\Psi_{q^{i+j}, F}$, and $f = g(x^{q^{k-i-j}})$. Then

(i) f is irreducible of degree $sq^{k-i-j}/\gcd(e, s)$.

(ii) If $p^q \not\equiv p \bmod q^2$, then $i = 1$, and f is an irreducible factor of $\Psi_{q^k, F}$ of degree $q^{k-j-1} \cdot deg g \geq q^{k-j-1}$.

(iii) If p is primitive modulo q^2, and $\gcd(e, (q-1)q) = 1$, then $f = \Psi_{q^k, F}$ is irreducible of degree $(q-1)q^{k-1}$.

Example 2.5. We explain for $q = 3$ the methods that we will propose in Section 5 for computing irreducible polynomials. Let $p \neq 3$ be a prime, $e, k \geq 1$, $F = GF(p^e)$, and $s = \mathrm{ord}_3(p)$. We will consider two cases:

Case 1: p is primitive mod 9 (so that $s = 2$) and $\gcd(e, 6) = 1$. The first condition is equivalent to $p \equiv 2$ or $5 \bmod 9$, and then $\Psi_{3^k, F} = x^{2 \cdot 3^{k-1}} + x^{3^{k-1}} + 1 \in F[x]$ is irreducible. (See van Lint [1971], Theorem 1.1.28, for $p = 2$, $e = 1$.)

Case 2: $p^3 \not\equiv p \bmod 9$ and $\gcd(e, 3s) = 1$. The first condition is equivalent to $p \not\equiv 1, 8 \bmod 9$. The primes not included in Case 1 satisfy $p \equiv 4$ or $7 \bmod 9$. In these two cases, $p \neq 2$, $s = 1$, -3 is a square modulo p, and

$$\Psi_{3,F} = \dot{x}^2 + x + 1 = (x - (-1+\sqrt{-3})/2) \cdot (x - (-1-\sqrt{-3})/2).$$

Then the factor

$$x^{3^{k-1}} - (-1+\sqrt{-3})/2 \in F[x]$$

of $\Psi_{q^k, F}$ is irreducible.

Example 2.6. We discuss the case $q = 2$ excluded in Corollary 2.4. We let $F = GF(p^e)$, and in view of Fact 2.1(iii), we assume that $2 \nmid e$ and $p \equiv 3$ or $5 \bmod 8$. If $p \equiv 5 \bmod 8$, then -1 is a square modulo p and 2 and -2 are non-squares. In this case,

$$\Psi_{4,F} = x^2+1 = (x-\sqrt{-1})\cdot(x+\sqrt{-1}),$$

and the factor

$$x^{2^{k-2}}-\sqrt{-1} \in F[x]$$

of $\Psi_{2^k,F}$ is irreducible for $k \geq 2$. If $p \equiv 3 \bmod 8$, then -2 is a square modulo p and -1 and 2 are non-squares. In this case,

$$\Psi_{8,F} = x^4+1 = (x^2+\sqrt{-2}\,x-1)\cdot(x^2-\sqrt{-2}\,x-1)$$

is an irreducible factorization, and

$$x^{2^{k-2}}+\sqrt{-2}\,x^{2^{k-3}}-1 \in F[x]$$

is an irreducible factor of $\Psi_{2^k,F}$ for $l \geq 3$. (Also, $\Psi_{4,F}$ is irreducible.)

The square roots required in these factorizations can be computed deterministically in polynomial time assuming the ERH (Huang [1985], Schoof [1985]).

3. Numbers of large order modulo q^l

Given a prime number p, we want to find a small prime number q such that p has large order modulo q^l, if l is large. We consider two variants of "large order": order at least q^{l-1} in this section, and maximal order $(q-1)q^{l-1}$ (for q odd) in Section 4.

In this section, a heuristic consideration leads to a conjecture asserting the existence of a small q. The conjecture is supported by numerical calculations, and we prove that the conjecture holds for randomly chosen primes. Corollary 2.4(ii) then provides large irreducible polynomials in $GF(p^e)$.

We consider

$$S = \{(p, q): p, q \text{ are prime numbers, } p \neq q \text{, and either}$$
$$(q \neq 2 \text{ and } p^q \not\equiv p \bmod q^2) \text{ or } (q = 2 \text{ and } p \equiv 3 \text{ or } 5 \bmod 8)\},$$

and for p prime and $x \in \mathbf{R}$

$$s(p) = \min\{q : (p, q) \in S\},$$

$$\sigma(x) = \min\{p : p \text{ prime and } \forall q \leq x \ (p, q) \notin S\}.$$

(If the set defining $s(p)$ is empty, set $s(p) = \infty$.) For $(p, q) \in S$, Corollary 2.4(ii) and Example 2.6 provide large irreducible polynomials in $GF(p^e)[x]$. s and σ are inverse functions in the following sense:

$$\forall p, x \ (\ p < \sigma(x) \iff \forall p' \leq p \ \ s(p') \leq x). \tag{3.1}$$

Also, σ is monotonely increasing.

In Section 5 we will want $s(p)$ to be small, say $O(\log\ p)$, or equivalently, $\sigma(q)$ to be large, say $\sigma(q) = \exp(\Omega(q))$.

Lemma 3.1. Let q be an odd prime.

(i) Let $1 \leq a < q^2$, and $a \equiv b \bmod q$ with $1 \leq b < q$. Then

$$a^q \equiv a \bmod q^2 \iff a \equiv b^q \bmod q^2.$$

(ii) There are exactly $q-1$ numbers a such that $1 \leq a < q^2$, $q \nmid a$ and $a^q \equiv a \bmod q^2$.

Proof. (i) Let $a = b + cq$ with $1 \leq b < q$, $0 \leq c < q$ be the q-adic expansion of a. Then

$$a^q = (b + cq)^q = \sum_{0 \leq j \leq q} \binom{q}{j} b^{q-j}(cq)^j \equiv b^q + qb^{q-1}cq \equiv b^q \bmod q^2.$$

Hence

$$a^q \equiv a \bmod q^2 \Longleftrightarrow a \equiv b^q \bmod q^2.$$

(ii) is clear.

For $x \in \mathbf{R}$, let

$$\alpha(x) = 2 \cdot \prod_{q \le x} q^2,$$

where the product is over the prime numbers up to x. By Lemma 3.1, for every odd prime q we have $q-1$ residue classes modulo q^2 (and 2 residue classes modulo 8, if $q = 2$) which contain prime numbers $p > q$ such that $(p, q) \notin S$. For any prime $p > x$, the question whether $(p, q) \notin S$ for all $q \le x$ depends only on the residue class of p modulo $\alpha(x)$, and there are

$$\beta(x) = 2 \prod_{q \le x} (q-1)$$

residue classes which contain such p's. If these residue classes are represented by $u_1(x),\ldots,u_{\beta(x)}(x)$ with

$$1 = u_1(x) < u_2(x) < \cdots < u_{\beta(x)}(x) < \alpha(x) < u_{\beta(x)+1}(x) = \alpha(x)+1,$$

then the average gap between $u_i(x)$ and $u_{i+1}(x)$ is

$$\gamma(x) = \frac{\alpha(x)}{\beta(x)} = \prod_{q \le x} \frac{q^2}{q-1}.$$

Note that $u_2(q) \le \sigma(q)$; in Remark 3.4 we give the $u_i(q) \le \sigma(q)$ for $q \le 13$.

We now conjecture that, in a logarithmic sense, $\sigma(x)$ (which is larger than the first gap $u_2(x) - 1$) is not much smaller than the average gap $\gamma(x)$.

Conjecture C_1. There exist $c, N > 0$ such that for all $x \ge N$

$$c \cdot \log \gamma(x) \le \log \sigma(x). \tag{3.2}$$

For polynomial-time algorithms in Section 5, $\log\sigma(x) = (\log\gamma(x))^{\Omega(1)}$ would suffice. Apart from the heuristic, we give three arguments supporting the conjecture: Table 1 shows that it holds for $x \le 23$, with $c = 0.98$, Theorem 3.6 shows that it holds for random primes, and a conjecture by Murata [1981] essentially implies C_1 (Proposition 3.8). The following lemma gives the order of magnitude conjectured for $\log \sigma(x)$. ("log" always means natural logarithm in this paper.)

Lemma 3.2. For $x > 1$

$$x - \frac{x}{\log x} < \log \gamma(x) < x + \frac{x}{\log x}.$$

Proof. For the upper bound on $\log \gamma(x)$, we have

$$\log \gamma(x) = \log \prod_{q \le x} q + \log \prod_{q \le x} \frac{q}{q-1}$$

$$\le x + \frac{x}{2 \log x} + \log(e^{C} \cdot \log x \cdot (1 + \frac{1}{\log^2 x}))$$

for $x > 1$, by Rosser & Schoenfeld [1962], (3.15) and (3.30), where $C \le 0.57722$ is Euler's constant. It is sufficient to show that

$$C + \log\log x + \log(1 + \frac{1}{\log^2 x}) \le \frac{1}{2} \frac{x}{\log x}$$

for $x \ge 7$, since the lemma is easily checked for $1 < x < 7$. One verifies that

$$6C \log x \le x,$$

$$3 \cdot \log x \cdot \log\log x \le x,$$

$$12 \cdot \log(1 + \frac{1}{\log^2 x}) \cdot \log x \le 12 \cdot \log(1 + \frac{1}{\log^2 7}) \log x \le x,$$

for $x \ge 7$. Together we get

$$C + \log\log x + \log(1 + \frac{1}{\log^2 x}) \le (\frac{1}{6} + \frac{1}{3} + \frac{1}{12}) \frac{x}{\log x} = \frac{1}{2} \frac{x}{\log x}.$$

One easily checks the lower bound for $x < 41$, and for $x \ge 41$

$$\log \gamma(x) \ge \log \prod_{q \le x} q \ge x - \frac{x}{\log x},$$

by Rosser and Schoenfeld [1962], (3.16).

Proposition 3.3. Conjecture C_1 holds if and only if there exist $c', N' > 0$ such that for all $y \ge N'$ we have

$$\forall p \le y \;\; s(p) \le c' \log y. \tag{3.3}$$

Proof. Let c, N be such that (3.2) holds for all $x \ge N$. We assume that $N \ge e^2$. Set $c' = 2/c$, $N' = \exp(cN/2)$, and let $y \ge N'$. Set $x = 2c^{-1} \log y$. Then $x \ge N \ge e^2$, and

$$\sigma(x) \ge \exp(c \log \gamma(x)) > \exp(c(x - \frac{x}{\log x})) \ge \exp(c\frac{x}{2}) = y.$$

Now let $p \le y$ be a prime. Then $p < \sigma(x)$, and by (3.1),

$$s(p) \le x = c' \log y.$$

For the reverse claim, let $c', N' > 0$ be such that (3.3) holds for all $y \ge N'$. We assume that $N' \geq 4$ and $c' \geq 2$; then $2c' \log(N'/2) \geq e$. Set

$$c = \frac{1}{4c'}, \quad N = 2c' \log \frac{N'}{2},$$

let $x \geq N$, and set $y = 2 \cdot \exp(2cx)$. Then $y \geq N'$. Let p be a prime number with $y/2 \leq p \leq y$; such a prime exists by Bertrand's postulate (Rosser & Schoenfeld [1962], (3.9)). Then

$$\forall p' \leq p \leq y \quad s(p') \leq c' \log y = c' \log 2 + \frac{x}{2} \leq x.$$

By (3.1), we have $p < \sigma(x)$, hence

$$\log \sigma(x) > \log p \geq \log \frac{y}{2} = 2cx \geq c\,(x + \frac{x}{\log x}) \geq c \, \log \gamma(x),$$

using that $x \geq e$ and Lemma 3.2.

The proof shows that if (3.3) holds with the values (c', N') (and $N' \geq 4$, $c' \geq 2$), then also with $(8c', (N'/2)^{1/4})$; hence also with $(c'(\log N')^{3/2}, 4)$.

Remark 3.4. For $q \leq 13$, we list the $u_i(q)$ with $1 \leq u_i(q) \leq \sigma(q)$.

$$u_2(2) = \sigma(2) = 7, \quad u_2(3) = \sigma(3) = 17,$$

$$u_2(5) = 143 = 11 \cdot 13 < u_3(5) = \sigma(5) = 199,$$

$$u_2(7) = 1{,}207 = 17 \cdot 71 < u_3(7) = 2{,}449 = 31 \cdot 79 < u_4(7) = 3{,}007 = 31 \cdot 97 <$$

$$u_5(7) = 3{,}743 = 19 \cdot 197 < u_6(7) = \sigma(7) = 4{,}049,$$

$$u_2(11) = 1{,}207 < u_3(11) = 4{,}607 = 17 \cdot 271 < u_4(11) = 19{,}601 = 17 \cdot 1153 <$$

$$u_5(11) = 22{,}049 = 17 \cdot 1297 < u_6(11) = 27{,}343 = 37 \cdot 739 <$$

$$u_7(11) = 30{,}007 = 37 \cdot 811 < u_8(11) = 49{,}607 = 113 \cdot 439 <$$

$$u_9(11) = \sigma(11) = 52{,}057,$$

$$u_2(13) = \sigma(13) = 132{,}857.$$

Table 1 shows x, $\sigma(x)$, and rounded values of $\gamma(x)$ and

$$\lambda(x) = \frac{\log \sigma(x)}{\log \gamma(x)},$$

for prime numbers $x \leq 23$. (Between two consecutive prime numbers, $\sigma(x)$ and $\gamma(x)$ are constant.) Note that $0.98 \leq \lambda(x) \leq 1.7$ for $x \leq 23$, so that (3.2) holds for $1 < x < 29$ and $c = 0.98$. (The values of $\sigma(x)$ have passed probabilistic primality tests; the true value of $\sigma(x)$ is at least the one given here.)

x	$\sigma(x)$	$\gamma(x)$	$\lambda(x)$
2	7	4	1.4037
3	17	18	0.9802
5	199	112.5	1.1208
7	4 049	918.8	1.2174
11	52 057	11 116.9	1.1657
13	132 857	156 562.7	0.9863
17	4 651 993	2 827 913.0	1.0335
19	256 899 943	56 715 365.9	1.0846
23	1 133 144 266 727 951	1 363 746 751.6	1.6480

Table 1.

We now prove that Conjecture C_1 holds for random prime numbers: for a random prime $p \le e^n$, we have $s(p) \le n$ with probability at least $1 - e^{-n/20}$.

As usual, we let $\theta(x) = \sum_{q \le x} \log q$, so that $\alpha(x) = 2\exp(2\theta(x))$.

Lemma 3.5. Let $x, y, z \in \mathbf{R}$ be such that

$$\alpha(x) = 2 \prod_{q \le x} q^2 < y < z,$$

and let

$$P(x, y, z) = \{p : p \text{ prime}, y \le p \le z, x < s(p)\}.$$

Then

$$\#P(x, y, z) \le \frac{2z}{\exp(\theta(x)) \cdot (\log y - \log(\alpha(x)))}.$$

Proof. As remarked in Lemma 3.1(ii), there are

$$\beta(x) = 2 \prod_{q \le x} (q - 1)$$

many residue classes a modulo $\alpha(x)$ such that every $p \in P(x, y, z)$ is congruent to some such a. Note that $\phi(\alpha(x)) = \beta(x)\exp(\theta(x))$. By the Prime Number Theorem for arithmetic progressions in Montgomery & Vaughan [1973], Theorem 2, we have

$$\#P(x, y, z) \le \frac{2\beta(x)(z - y)}{\phi(\alpha(x)) \log(\dfrac{y}{\alpha(x)})} \le \frac{2z}{\exp(\theta(x))(\log y - \log(\alpha(x)))}.$$

Theorem 3.6. Let $z \geq e^2$. Then for a random prime number p with $2 \leq p \leq z$ we have

$$\text{prob}(s(p) > \log z) \leq z^{-1/20}.$$

Proof. We let

$$\eta(z) = \#\{p : 2 \leq p \leq z, p \text{ prime, and } s(p) > \log z\} \cdot \pi(z)^{-1}$$

be the probability in question, and prove

$$\eta(z) \leq z^{-1/20}$$

by induction on $\lceil z \rceil$. The inductive step assumes $z \geq 10^{10}$. The claim was verified for smaller values of z computationally, as follows. If q is a prime and q^+ the next prime, let

$$\delta(q) = \#\{p : p < \exp(q^+) \text{ and } q^+ \leq s(p)\}.$$

Then, if

$$\delta(q) \leq q^{-1}\exp(q - q^+/20), \tag{3.4}$$

we have for $\exp(q) \leq z < \exp(q^+)$

$$\text{prob}(s(p) > \log z) = \text{prob}(s(p) \geq q^+) \leq \frac{\delta(q)}{\pi(\exp(q))} \leq$$
$$\frac{q\,\delta(q)}{\exp(q)} \leq \exp(-q^+/20) \leq z^{-1/20}.$$

(3.4) was verified for $q \leq 19$, and we now assume $z \geq 10^{10}$. (For $e^{23} < 10^{10} \leq z \leq 10^{15} < \sigma(23)$, we have $\text{prob}(s(p) > \log z) = 0$.) We denote by ϵ, λ, μ, ν parameters that we will fix later. We let $y = z^{\epsilon}$, $x = \epsilon\lambda \log z$, and assume that the following hold:

$$\epsilon\lambda \leq 1. \tag{3.5}$$

$$\frac{1}{2}\log 2 + \theta(x) \leq \mu x \text{ for } 5 \leq x, \tag{3.6}$$

$$\nu x \leq \theta(x) \text{ for } 5 \leq x, \tag{3.7}$$

$$y \leq z - 1, \tag{3.8}$$

$$113.6 \leq \alpha(x) < y, \tag{3.9}$$

$$5 \leq x. \tag{3.10}$$

Splitting the primes up to z into those up to y and those greater than y, we have

$$\eta(z) \leq \eta(y) \cdot \pi(y) \cdot (\pi(z))^{-1} + \#P(x, y, z) \cdot (\pi(z))^{-1}$$

$$
\begin{aligned}
&\leq y^{-1/20} \cdot \frac{5}{4} \cdot \frac{z^{\epsilon}}{\epsilon \log z} \cdot (\frac{z}{\log z})^{-1} \\
&\quad + \frac{2z}{\exp(\theta(x))} \cdot (\log y - \log(\alpha(x))) \\
&= \frac{5}{4\epsilon} z^{-\epsilon/20+\epsilon-1} + \frac{2\log z}{\epsilon\log z - \log 2 - 2\theta(x)} \cdot \exp(-\theta(x)) \\
&\leq \frac{5}{4\epsilon} z^{19\epsilon/20-1} + \frac{2}{\epsilon} \cdot \frac{1}{1-2\lambda\mu} \cdot \exp(-\nu x) \\
&= \frac{5}{4\epsilon} z^{19\epsilon/20-1} + \frac{2}{\epsilon} \frac{1}{1-2\lambda\mu} z^{-\epsilon\lambda\nu},
\end{aligned}
$$

where we have used Lemma 3.5 and Rosser & Schoenfeld [1962], (3.5) and (3.7). Now we use the following values:

$$\lambda = \frac{1}{3}, \ \mu = \frac{14}{13}, \ \nu = 0.4858 \ (<\theta(5)/7),$$

and ϵ such that

$$\frac{19}{20}\epsilon - 1 = -\epsilon\lambda\nu$$

(so that $\epsilon = 0.89933...$). We check (3.5) through (3.10): A table shows that (3.6) holds for $x \leq 695$, and for $x > 695$, Rosser & Schoenfeld (3.15) implies that

$$\theta(x) \leq x + \frac{x}{2}\log x \ \leq x + \frac{x}{13} - \frac{1}{2}\log 2.$$

Similarly, one verifies (3.7) for $x \leq 41$, and otherwise uses

$$\theta(x) \geq x - \frac{x}{\log} x \geq \nu x,$$

by Rosser & Schoenfeld (3.16). For the second inequality of (3.9) we have

$$\alpha(x) \doteq 2\exp(2\theta(x)) \leq \exp(2\mu x) = z^{2\epsilon\lambda\mu} < z^{\epsilon} = y.$$

Thus

$$\eta(z) \leq (\frac{5}{4\epsilon} + \frac{2}{3}\frac{1}{1-2\lambda\mu}) z^{-\epsilon\lambda\mu} \leq 3.8 \, z^{-0.14} \leq z^{-1/20}.$$

Example 3.7. Of the 460 primes p between 32 633 and 2^{64} in Table 4.5.4-1 of Knuth [1981] (which were certainly not chosen with a view to favoring Conjecture C_1), $220 = 47.83\%$ have $s(p)=2$; for random primes, say up to 2^{64}, one expects 50% to have this property. In the table, $159 = 34.57\%$ have $s(p)=3$ (expected 33.33%), $67 = 14.57\%$ have $s(p)=5$ (expected 13.33%), and the remaining $14 = 3.04\%$ have

$s(p)=7$ (expected 2.86%). For all these p, $s(p)<\log p$. (0.48% are expected to have $s(p)\geq 11$.)

Rosser [1941] shows the following connection of our set S with Fermat's conjecture: if $(p,q)\in S$, $q\geq 3$ and $p\leq 43$, then there exist no $x,y,z\in \mathbf{Z}$ such that $\gcd(xyz,q)=1$ and $x^q+y^q=z^q$.

Consider the set

$$F_a(x)=\{q: q \text{ prime}, 3\leq q\leq x, q \nmid a, \text{and } a^q\equiv a \bmod q^2\}$$

for $a\in\mathbf{Z}$, $x\in\mathbf{R}$. When p is prime, then

$$F_p(x)=\{q: q\neq p \text{ prime}, 3\leq q\leq x, (p,q)\notin S\}.$$

Murata [1981], Theorem 1, implies that for $x\geq 286$ and a random integer a between 2 and x^4

$$\mathrm{prob}(\#F_a(x)>2\log\log x)\leq 2(\log\log x)^{-½}.$$

Since $2\log\log x<\pi(x)$ for $x\geq 2$, this implies that

$$\mathrm{prob}(\forall q\leq 2\log\log x \quad p^q\equiv p \bmod q^2))\leq 2(\log\log x)^{-½}.$$

Compared with Theorem 3.6, this yields a smaller bound on the smallest q, but the probability decreases much slower. Murata also conjectures that

$$\#F_a(x)\sim D_a \log\log x$$

for large x, with a constant D_a depending on a. We show that with small D_a (say, $D_a=O(\log a)$), the upper bound would essentially imply Conjecture C_1.

Proposition 3.8. Let p be a prime, and $D\in\mathbf{R}$ such that

$$\forall x\geq 3 \quad \#F_p(x)\leq D\log\log x,$$

and assume that $D\geq 8$. Then

$$s(p)\leq 4D\log D\log\log D.$$

Proof. Let $x=4D\log D\log\log D$. Then

$$\log x\leq \log D+\log(4\log D\log\log D)\leq 2\log D,$$

$$\log\log x\leq \log 2+\log\log D\leq 2\log\log D.$$

Thus

$$D=\frac{x}{2\log D\cdot 2\log\log D}\leq\frac{x}{\log x\log\log x}<\frac{\pi(x)}{\log\log x}$$

by Rosser and Schoenfeld [1962], (3.5). Now

$$\pi(x) > D \ \operatorname{loglog} x \ \geq \#F_p(x)$$

implies that $s(p) \leq x$.

4. Primitive elements modulo q^k

This section parallels the previous one, now with a view to applying Corollary 2.4(iii). Thus we consider

$$T = \{(p, q) \colon p, q \text{ prime}, q \geq 3, \text{ and } p \text{ is primitive modulo } q^2\},$$

and for p prime and $x \in \mathbf{R}$

$$t(p) = \min\{q : (p, q) \in T\}.$$

$$\tau(x) = \min\{p : p \text{ prime, and } \forall q \leq x \ (p, q) \notin T\},$$

Then

$$\forall p, x \quad (p < \tau(x) \Longleftrightarrow \forall p' \leq p \quad t(p') \leq x). \tag{4.1}$$

Lemma 4.1. Let $q \geq 3$ be prime. There are exactly $(q-1)(q-\phi(q-1))$ integers a such that $1 \leq a < q^2$, $q \nmid a$, and a is not primitive modulo q^2.

Proof. Using Fact 2.1(ii) and Lemma 3.1, we have

$$\begin{aligned} &\#\{a : 1 \leq a < q^2, q \nmid a, \text{ and } a \text{ not primitive mod } q^2\} \\ &\quad = \#\{a : 1 \leq a < q^2, q \nmid a, a \text{ not primitive mod } q\} \\ &\quad + \#\{a : 1 \leq a < q^2, q \nmid a, a \text{ primitive mod } q, \\ &\qquad\quad \text{and } a^q \equiv a \text{ mod } q^2\} \\ &\quad = q \cdot (q-1-\phi(q-1)) + \phi(q-1) = (q-1)(q-\phi(q-1)). \end{aligned}$$

Remark 4.2. The numerical evidence exhibited below indicates that the direct ana log ue of Conjecture C_1 is probably false. The ana log ue would state that

$$c \cdot \log \gamma^*(x) \leq \log \tau(x),$$

where

$$\gamma^*(x) = \prod_{3 \leq q \leq x} \frac{q^2}{(q-1)(q-\phi(q-1))}.$$

However, using

$$\phi(q-1) \geq \frac{q-1}{\text{loglog}(q-1)} \geq \frac{q}{2\ \text{loglog}q} \geq \frac{q}{2\ \text{loglog}x}$$

for $q \leq x$ and x large enough, it follows that asymptotically

$$\log \gamma^*(x) = \Omega(x/(\log x\ \text{loglog}x)),$$

but $\log(\tau(x))$ seems to grow much slower.

Numerical evidence suggests the following conjecture.

Conjecture C_2. There exists c , $N > 0$ such that for all $x \geq N$

$$cx^2 \leq \tau(x). \tag{4.2}$$

Proposition 4.3. Conjecture C_2 holds if and only if there exist c', $N' > 0$ such that for all $y \geq N'$

$$\forall p < y \quad t(p) \leq c' y^{1/2}. \tag{4.3}$$

Proof. Taking c and N satisfying C_2, we set $N' = cN^2$ and $c' = c^{-1/2}$. Then for $y \geq N'$, we set $x = c' y^{1/2} \geq N$. For any $p < y$ we have $p < y = cx^2 \leq \tau(x)$, hence $t(p) \leq x$ by (4.1).

For the reverse implication, we set $c = (c')^{-2}$ and $N = c'(N')^{1/2}$. Then if $x \geq N$, we let $y = cx^2 \geq N'$. For any prime $p < y$, $t(p) \leq c' y^{\frac{1}{2}} = x$, and hence $\tau(x) \geq y = cx^2$.

Conjecture C_2 has the following relation with Artin's conjecture. Set

$$T^* = \{(a, q) \in \mathbf{Z}^2 \colon q \geq 3 \text{ is prime, and } a \text{ is primitive modulo } q\},$$

and for $a \in \mathbf{Z}$,

$$T_a^* = \{q : (a, q) \in T^*\},$$

$$t^*(a) = \min T_a^*,$$

with $t^*(a) = \infty$ if $T_a^* = \emptyset$; e.g. when a is a perfect square. For a prime p, $t^*(p) \leq t(p)$. Artin's conjecture gives the following density for T_a^*:

$$\#\{q \in T_a^* \colon q \leq x\} \sim C(a)\pi(x),$$

where $C(a)$ is a constant depending on a, and a is neither -1 nor a perfect square. Hooley [1967] proves this conjecture, assuming the ERH. Let

$$C = \prod_{p \text{ prime}} (1 - \frac{1}{p(p-1)}) = 0.3739558....$$

Then for a prime p , Hooley's result is

$$C\,(p\,) = \begin{cases} C & \text{if } p \equiv 3 \bmod 4, \\ C \cdot (1 + \dfrac{1}{p^{2} - p - 1}) & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

For Table 2, the 27 prime numbers q up to 103 were examined. For the given ranges of x , the table contains ranges of $\delta(x\,) = \dfrac{\tau(x\,)}{x^{2}}$. Note that Conjecture C_{2} states that $\delta(x\,) = \Omega(1)$. E.g., the last line of Table 2 implies that for all primes $p \leq 80{\cdot}103^{2}$ we have $t\,(p\,) \leq p^{1/2}$. In fact, $t\,(109){=}13$, and for all other primes p considered, i.e. $109 < p \leq 9\,188\,941 = \tau(103)$, we have $t\,(p\,) \leq p^{1/2}$.

x	$\delta(x\,)$
$19{\leq}x{\leq}50$	$1{\leq}\delta(x\,){\leq}12$
$50{\leq}x{\leq}79$	$5{\leq}\delta(x\,){\leq}150$
$79{\leq}x{\leq}103$	$80{\leq}\delta(x\,){\leq}1000$

Table 2.

Again, the conjecture holds for random primes.

Theorem 4.4. For $z \in \mathbf{R}$ sufficiently large, and p a random prime not larger than z , we have

$$\text{prob}(\,t\,(p\,) > z^{1/2}) = O\,(z^{-1/2}\,(\log z\,)^{7/5}).$$

Proof. We have

$$\text{prob}(\,t\,(p\,) > z^{1/2}) \leq \text{prob}(\,t^{\,*}(p\,) > z^{1/2}) + \text{prob}(\,s\,(p\,) > z^{1/2}).$$

Warlimont [1972] proves that for large z

$$\#\,\{a \in \mathbf{Z}\colon 1{\leq}a\leq z \text{ and } t^{\,*}(a\,) > z^{1/2}\} = O\,(z^{1/2}\,(\log z\,)^{2/5}),$$

so that the first summand above is

$$O\,(\frac{z^{1/2}\,(\log z\,)^{2/5}}{\pi(z\,)}) = O\,(z^{-1/2}\,(\log z\,)^{7/5}).$$

For the second summand, it is sufficient to consider a single prime q with $z^{1/2}/2e \leq q \leq z^{1/2}/e$. It follows from Lemma 3.1(ii) and Montgomery & Vaughan [1973], Theorem 2, that

$$\# \{p : q < p \le z \text{ and } (p,q) \in S\} \le \frac{2z}{\phi(q^2)\log(z/q^2)} \cdot (q-1) \le \frac{2z}{q/2} \le 8ez^{1/2},$$

so that a coarse estimate is

$$\mathrm{prob}(s(p) > z^{1/2}) \le (\pi(q) + 8ez^{1/2})/\pi(z) = O(z^{-1/2}\log z).$$

Example 4.5. All 460 primes considered in Example 3.7 have $t(p) \le 41 \le p^{1/2}$.

5. Computing irreducible polynomials

We show how to find irreducible polynomials of large degree over finite fields fast, assuming the conjectures of sections 3 and 4.

The sum, product, quotient and remainder, and gcd of two polynomials in $F[x]$ of degree at most d can be computed with $O(d \log d)$ operations in $F = \mathbf{Z}_p[t]/(h) = GF(p^e)$ (Aho, Hopcroft & Ullman [1974]). Similarly, an operation $(+, *, /)$ in F can be performed in $O(e \log e)$ operations in $\mathbf{Z}_p$, and an operation in $\mathbf{Z}_p$ in $O(\log p \operatorname{loglog} p \operatorname{logloglog} p)$ bit operations. Here we assume the standard representations of $f \in F[x]$ by its coefficients, $a \in F$ by $(a_0, \ldots, a_{e-1}) \in \mathbf{Z}_p^e$ such that $a = (\sum_{0 \le i < e} a_i t^i \bmod h)$, and of $b \in \mathbf{Z}_p$ by the binary representation of $b^* \in \mathbf{Z}$ such that $b = (b^* \bmod p)$ and $0 \le b^* < p$.

If F is a field, then $M_F : \mathbf{N} \rightarrow \mathbf{R}$ is such that the product of two $n \times n$-matrices over F can be computed in $O(M_F(n))$ operations in F. We can choose $M_F(n) = n^{2.496} < n^{2.5}$ (Coppersmith and Winograd [1982]). In order to be able to neglect logarithmic terms, we use the following notation (generalizing Definition 6.4 in von zur Gathen [1985a]).

Definition 5.1. Let $r \in \mathbf{N}$, and $s, t : \mathbf{N}^r \rightarrow \mathbf{R}_{\geq 0}$. Then $s = 0^*(t)$ if and only if there exist $k, m \in \mathbf{N}$ such that

$$\forall n_1, \ldots, n_r \geq m \quad s(n_1, \ldots, n_r) \leq t(n_1, \ldots, n_r) \cdot (\log_2(2 + t(n_1, \ldots, n_r)))^k .$$

Thus $s = O^*(t)$ if and only if $s = O(t \cdot \log(2+t)^k)$ for some k.

We will use the following well-known facts.

Fact 5.2. Let p be a prime number, $d \geq 1$, and $F = \mathbf{Z}_p$.

(i) If $f \in F[x]$ has degree d, then the irreducible factorization of f can be computed by a deterministic algorithm with $O^*(M_F(d) + pd^2)$ operations in F.

(ii) If $f \in F[x]$ has degree d, then the irreducible factorization of f can be computed by a probabilistic (Las Vegas) algorithm with an expected number of $O^*(d^3 \log p)$ operations in F, and $O(d \log p)$ random bit choices.

(iii) If $d \geq 1$, then an irreducible monic polynomial in $F[x]$ of degree d can be found by a probabilistic algorithm with an expected number of $O^*(d^3 \log p)$ operations in F, and $O(d \log p)$ random bit choices.

(iv) If $p = 2$ and $n \geq 1$, then an irreducible polynomial of degree d with $n \leq d \leq 3n$ can be computed deterministically with $O(n)$ bit operations.

(v) If we assume an appropriate Extended Riemann Hypothesis (ERH), then any cyclotomic polynomial in $F[x]$ can be factored in deterministic polynomial time.

Proof. The algorithms proving these facts go back to Berlekamp [1967, 1970], see also Knuth [1981], 4.6.2, and Cantor & Zassenhaus [1981]. (ii) and (iii) are in Rabin [1980]. For (iv), see Example 2.5. (v) is proven in Huang [1985].

The algorithms extend easily to non-prime finite fields; see Cantor & Zassenhaus [1981] and von zur Gathen [1984].

Fact 5.3. Let $F = GF(p^e)$, and $f \in F[x]$ of degree d. Then an irreducible factor of f can be found with the following number of operations in $\mathbf{Z}_p$.

(i) With $O(M_{\mathbf{Z}_p}(de) + pd^2e \log(e+1) \log p)$ or $O^*((de)^{2.5} + d^2ep)$ operations by a deterministic algorithm.

(ii) With an expected number $O(M(de) + d^2e \log d \log(e+1) \log p)$ or $O^*((de)^{2.5} + d^2e \log p)$ operations by a Las Vegas algorithm.

Lemma 5.4. Let p be a prime number.

(i) If Conjecture C_1 holds, then one can find a prime number q such that $(p, q) \in S$ in $O^*(\log^2 p)$ bit operations.

(ii) If Conjecture C_2 holds, then one can find a prime number q such that $(p, q) \in T$ in $O^*(p^{3/4})$ bit operations.

Proof. (i) For any integer $q \geq 3$, one can test whether $(p, q) \in S$, i.e. whether q is prime, $p \neq q$ and $p^q \not\equiv p \bmod q^2$, in

$$O(q^{½} \log^2 q + \log p \cdot \log q + \log q \cdot \log^2 q)$$

bit operations. The first summand is for a trivial deterministic primality test, the second for $u = p \bmod q^2$ with $1 \leq u \leq q^2$, and the third for $u^q \bmod q^2$ (Aho, Hopcroft & Ullman [1974]). For $q = 2$, one can test $p \equiv 3$ or $5 \bmod 8$ in $O(\log p)$ bit operations. Under Conjecture C_1, there exists q such that $(p, q) \in S$ and $q = O(\log p)$ (Proposition 3.3), and the total cost for finding the smallest such q is $O^*(\log^2 p)$.

(ii) For $q \geq 3$, one can test whether $(p, q) \in T$ with the cost as above, plus the cost for testing whether p is primitive modulo q. This can be done by computing the distinct prime factors $q_1, \ldots, q_r$ of $q - 1$ in $O^*(q^{½})$ bit operations (by a trivial factoring algorithm) and testing whether

$$p^{(q-1)/q_i} \not\equiv 1 \bmod q$$

for $1 \leq i \leq r$, in $O(\log^3 q)$ bit operations. Under Conjecture C_2, there exists a

$q = O(p^{½})$ with $(p, q) \in T$, and the total cost for finding the smallest such q is $O^*(p^{3/4})$.

Theorem 5.5. Let p be a prime number, $e, n \geq 1$, and $F = GF(p^e)$. Then one can find an irreducible polynomial in $F[x]$ of some degree d such that $n \leq d$ by deterministic algorithms of the following running times.

(i) If Conjecture C_1 and ERH hold, with $(e \log p)^{O(1)} + O(ne \log^3 p)$ bit operations; then $d = O(n \log^2 p)$.

(ii) If Conjecture C_1 holds, with $O^*(e^5 + e^3 p + ne \log^3 p)$ bit operations; then $d = O(n \log^2 p)$.

(iii) If Conjecture C_2 holds and $e = 1$, with $O^*(p^{3/4} + p^{½} n)$ bit operations; then $d = O(p^{1/2} n)$.

Proof. For (i), find q with $(p, q) \in S$ and $q = O(\log p)$ as in Lemma 5.4(i). If q is odd, let $s = \text{ord}_q(p)$ and $q^j \| e$. Use Fact 5.2(v) to compute an irreducible factor $g \in F[x]$ of $\Psi_{q^{j+1},F}$ in $(e \log p)^{O(1)}$ bit operations, since $\deg \Psi_{q^{j+1}} = (q-1)q^j = O(e \log p)$. Set $k = j + 1 + \lceil \log_q n \rceil$, compute $f = g(x^{q^{k-j-1}}) \in F[x]$ in $O(ne \log^3 p)$ bit operations, and return f. Then f is irreducible by Corollary 2.4(ii), and

$$n \leq q^{k-j-1} \leq \deg f = sq^{k-j-1}/\gcd(e, s) \leq (q-1)q^{k-j-1} \leq q^2 n = O(n \log^2 p).$$

If $q = 2$ and $2 \not| e$, use the factorizations of $\Psi_{4,F}$ or $\Psi_{8,F}$ and appropriate substitutions, as in Example 2.6. If $2^j \| e$, then factorizations of $\Psi_{2^{j+3},F}$ are sufficient.

For (ii), find q, k, j as in (i), and use Fact 5.3(i) to compute an irreducible factor g of $\Psi_{q^{j+1},F}$, with $O^*(e^2 \log p)^{2.5} + e^3 \log^2 p \cdot p)$ or $O^*(e^5 + e^3 p)$ bit operations. Then proceed as in (i).

For (iii), use Lemma 5.4(ii) to find q with $q = O(p^{½})$ and $(p, q) \in T$ and set $k = 1 + \lceil \log_q (n/(q-1)) \rceil$. By Corollary 2.4(iii), $\Psi_{q^k,F} \in F[x]$ is irreducible of degree $d = (q-1)q^{k-1}$, and

$$n \leq d \leq qn = O(p^{1/2} n).$$

Remark 5.6. Assuming the ERH, it follows from the proof in Hooley [1967] that most $q \leq x$ for which p fails to be primitive are such that $p^{(q-1)/q_i} \equiv 1 \bmod q$ for a prime divisor $q_i \leq \frac{1}{6} \log x$ of $q-1$. If this asymptotic density result already applies to small values of x, then in the search for q with p primitive modulo q one will only rarely have to compute large prime factors of $q - 1$.

One advantage of the present method lies in the fact that given $F = GF(p^e)$ with a prime p, one only has to find some q with $(p, q) \in S$ resp. $(p, q) \in T$ (and $\gcd(e, (q-1)q) = 1$ and in order to find irreducible polynomials over F of arbitrarily large degree. The computation of such a q (and the factorization of $\Psi_{q^{j+1},F}$ if $(p,q) \in S$ and $q^j \,||\, e$) may be considered as a preprocessing stage, and e.g. for the computational model of P-uniform arithmetic networks over F, one can hard-wire such a q.

Corollary 5.7. If preprocessing depending on p is allowed for free and Conjecture C_1 holds, then one can find an irreducible polynomial in $\mathbf{Z}_p[x]$ of degree at least n with $O(n \log p)$ bit operations by a deterministic algorithm.

The computing time for Corollary 5.7 is proportional to the dense output size. This is the appropriate model if later on one wants to compute in the field $F[x]/(f)$. However, one may also consider more succinct representations such as sparse, formulas or straight-line programs. (See von zur Gathen [1985a] for such representations for multivariate polynomials.) If the representation by a straight-line program is allowed, then the simple expression given by Fact 2.2 shows that Corollary 5.7 holds even with $O(\log n + \log\log p)$ bit operations.

For practical purposes, the easiest implementation might be a deterministic search for q with $(p,q) \in S$ and a Las Vegas computation of an irreducible factor g of $\Psi_{q^{j+1},F}$ as preprocessing stages (where $q^j \,||\, e$), which then yields an irreducible polynomial $g(x^{q^k}) \in GF(p^e)[x]$ for any $k \geq 0$.

For the applications mentioned in the Introduction, one might actually just find the smallest q with $(p,q) \in S$, and then work in the extension ring $R = F[x]/(\Psi_{q^k,F})$ for sufficiently large k. If during the computation in R a division by a zero-divisor is attempted, this will provide a factorization $g_1 \cdot g_2 = \Psi_{q^k,F}$. Then the computation is continued in $R/(g_i)$ for $i = 1$ or $i = 2$. This approach will save the cost of factoring.

Acknowledgement

Many thanks go to Wolfgang Küchlin and Ronald Peikert, ETH Zürich, who helped with the computations.

References

L. Adleman and H.W. Lenstra, Finding irreducible polynomials over finite fields. To appear in Proc. 18th Ann. ACM Symp. Theory of Computing, Berkeley CA, 1986.

A.V. Aho, J.E. Hopcroft and J.D. Ullman, The design and analysis of computer algorithms. Addison-Wesley, Reading MA, 1974.

E.R. Berlekamp, Factoring polynomials over finite fields. Bell System Tech. J. **46** (1967), 1853-1859.

E.R. Berlekamp, Factoring polynomials over large finite fields. Math. Comp. **24** (l970), 713-735.

S.I. Borevich and I.R. Shafarevich, Zahlentheorie. Birkhäuser Verlag, Basel, 1966.

P. Camion, A deterministic algorithm for factorizing polynomials of $F_q\,[x\,]$. Ann. Discr. Math. **17** (1983), 149-157.

D.G. Cantor and H. Zassenhaus, On algorithms for factoring polynomials over finite fields. Math. Comp. **36** (1981), 587-592.

A.L. Chistov and D.Yu. Grigoryev, Polynomial-time factoring of the multivariable polynomials over a global field. LOMI preprint E-5-82, Leningrad, 1982.

D. Coppersmith and S. Winograd, On the asymptotic complexity of matrix multiplication. SIAM J. Comput. **11** (1982), 472-492.

W. Eberly, Very fast parallel matrix and polynomial arithmetic. Proc. 25th Ann. IEEE Symp. Foundations of Computer Science, Singer Island FL, 1984, 21-30.

J. von zur Gathen, Parallel algorithms for algebraic problems. SIAM J. Comput. **13** (1984), 802-824.

J. von zur Gathen [1985a], Irreducibility of multivariate polynomials. J. Computer System Sciences **31** (1985), 225-264.

J. von zur Gathen [1985b], Factoring polynomials and primitive elements for special primes. Manuscript, April 1985.

J. von zur Gathen and E. Kaltofen [1985a], Factorization of multivariate polynomials over finite fields. Math. Comp. **45** (1985), 251-261.

J. von zur Gathen and E. Kaltofen [1985b], Factoring sparse multivariate polynomials. J. Computer System Sciences **31** (1985), 265-287.

G.H. Hardy and E.M. Wright, An introduction to the theory of numbers. Clarendon Press, Oxford, 1962.

H. Hasse, Number Theory. Grundlehren der math. Wiss., vol. 229, Springer Verlag, 1980.

C. Hooley, On Artin's conjecture. J. reine ang. Math. **225** (1967), 209-220.

M.A. Huang, Riemann Hypothesis and finding roots over finite fields. Proc. 17th Ann. ACM Symp. Theory of Computing, Providence RI, 1985, 121-130.

E. Kaltofen, Deterministic irreducibility testing of polynomials over large finite fields. Manuscript, 1985.

D.E. Knuth, The Art of Computer Programming, Vol.2, 2nd Ed. Addison-Wesley, Reading MA, 1981.

A.K. Lenstra, Factoring multivariate polynomials over finite fields. J. Computer System Sciences **30** (1985), 235-248.

R. Lidl and H. Niederreiter, Finite fields. Encyclopedia of Mathematics and its applications, Vol. 20, Addison-Wesley, Reading MA, 1983.

J.H. van Lint, Introduction to coding theory. Graduate texts in Mathematics 86, Springer Verlag, New York, 1971.

H.L. Montgomery and R.C. Vaughan, The large sieve. Mathematika **20** (1973), 119-134.

L. Murata, An average type result on the number of primes satisfying generalized Wieferich condition. Proc. Japan Acad. **57** (1981), 430-432.

M.O. Rabin, Probabilistic algorithms in finite fields. SIAM J. Comp. **9** (1980), 273-280.

B. Rosser, An additional criterion for the first case of Fermat's last theorem. Bull. Amer. Math. Soc. **47** (1941), 109-110.

J.B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers. Ill. J. Math. **6** (1962), 64-94.

R.J. Schoof, Elliptic curves over finite fields and the computation of square roots mod p. Math. Comp. **44** (1985), 483-494.

R. Warlimont, On Artin's conjecture. J. London Math. Soc. **5** (1972), 91-94.

TECHNICAL REPORTS

#1-#72: not available

Number	Author	Title
* 73	Lucio F. Melli	The 2.pak Language: Primitives for AI Applications
* 74	David G. Kirkpatrick	Topics in the Complexity of Combinatorial Algorithms
* 75	Gerald A. Gorelick	A Complete Axiomatic System for Proving Assertions about Recursive and Non-Recursive Programs
* 76	Richard B. Bunt	Self-Regulating Schedulers for Operating Systems
* 77	James F. Allen	A Prototype Speech Understanding System
* 78	Alexander T. Borgida	Topics in the Understanding of English Sentences by Computer
* 79	Stephen A. Cook	Axiomatic and Interpretive Semantics for an Algol Fragment
* 80	Norman I. Badler	Temporal Scene Analysis: Conceptual Descriptions of Object Movements
* 81	R.A. Bedet W.H. Enright & T.E. Hull	Stiff Detest: A Program for Comparing Numerical Methods for stiff Ordinary Differential Equations
* 82	Derek C. Oppen	On Logic and Program Verification
83	Patrick Keast	The Evaluation of One-dimensional Quadrature Routines
* 84	Harry K.T. Wong	Generating English Sentences from Semantic Structures
* 85	Walter Berndl	An Analysis of the SPITBOL System

* Not available - may be obtained at a cnarge through:
Interlibrary Loans Section
Science and Medicine Library
University of Toronto
Toronto, Canada M5S 1A5

TECHNICAL REPORTS
(continued)

Number	Author	Title
* 86	Eshrat Arjomandi	A Study of Parallelism in Graph Theory
* 87	Robert A. Reckhow	On The Lengths of Proofs In The Propositional Calculus
88	Martin J. Dowd	Primitive Recursion Arithmetic With Recursion On Notation And Boundedness
89	L.W. Jackson & R.D. Skeel	Convergence And Stability Of Nordsieck Methods
* 90	Corot C. Reason	A Bi-Directional Speech Parsing Technique
* 91	Grant A. Cheston	Incremental Algorithms in Graph Theory
* 92	Peter B. Gibbons	Computing Techniques for the Construction and Analysis of Block Designs
* 93	John K. Tsotsos	A Prototype Motion Understanding System
94	L.W. Jackson	The Computation of Coefficients of Variable-Step Adams Methods
*95	Stephen A. Cook	Soundness and Completeness of an Axiom System for Program Verification
* 96	G. Fairweather & P. Keast	A Comparison of Non-Adaptive Romberg Quadrature Routines
* 97	Charles Rackoff	The Covering and Boundedness Problems for Vector Addition Systems
*98	W.H. Enright	Improving the Efficiency of Matrix Operations in the Numerical Solution of Stiff ODE's

* Not available - may be obtained at a charge through:
Interlibrary Loans Section
Science and Medicine Library
University of Toronto
Toronto, Canada M5S 1A5

TECHNICAL REPORTS
(continued)

Number	Author	Title
*99	Daniel Brand	Proving Programs Incorrect
*100	T.E. Hull W.H. Enright K.R. Jackson	User's Guide for DVERK - a Subroutine for Solving Non-stiff ODE's
*101	K.R. Jackson W.H. Enright T.E. Hull	A Theoretical Criterion for Comparing Runge-Kutta Formulas
*102	R.L. Johnston C. Addison	STUNT - Software for Teaching Undergraduates Numerical Techniques
*103	Pavol Sermer	Finite Element Methods in the Numerical Solution of Mixed-Type Partial Differential Equations
* 104 (2nd ed.)	Nicholas D. Roussopoulos	A Semantic Network Model of Data Bases
*105	Hector J. Levesque	A Procedural Approach to Semantic Networks
*106	Manfred Maier	Some Numerical Results from the Study of Steady Fluid Flow
*107	Robin Cohen	Computer Analysis of Temporal Reference
*108	Mary Katherine Horrigan	Modelling Simple Dialogs
* 109	Stephen A. Cook Robert A. Reckhow	The Relative Power of Propositional Proof Systems
* 110	R.L. Johnston Rudolph Mathon	The Computation of Electric Dipole Fields in Conducting Media
* 111	W.H. Enright	The Efficient Solution of Linear Constant Coefficient Systems of ODEs
* 112	Alexander T. Borgida	Formal Studies of Stratificational Grammars
*113	Patrick W. Dymond	Complexity Relationships among some Models of Computation

* Not available - may be obtained at a charge through:
Interlibrary Loans Section
Science and Medicine Library
University of Toronto
Toronto, Canada M5S 1A5

TECHNICAL REPORTS
(continued)

Number	Author	Title
*114	Leslie M. Goldschlager	Synchronous Parallel Computation
*115	Peter F. Schneider	Organization of Knowledge in a Procedural Semantic Network Formalism
*116	P. Keast	Families of s-Dimensional, Degree 2t+1 Quadrature Rules for Product Spaces
*117	Stephen A. Cook and Charles W. Rackoff	Space Lower Bounds for Maze Threadability on Restricted Machines
*118	Philip R. Cohen	On Knowing What to Say: Planning Speech Acts
*119	Michael Anthony Bauer	A Basis for the Acquisition of Procedures
*120	R. Aleliunas	A Simple Graph Traversing Problem
*121	K.R. Jackson and R. Sacks-Davis	An Alternative Implementation of Variable Stepsize Multistep Formulas for Stiff ODEs
*122/78	Martin Tompa	Time-Space Tradeoffs for Straight-line and Branching Programs
*123/78	C.J. Colbourn	A Bibliography of the Graph Isomorphism Problem
*124/78	Stephen A. Cook	Deterministic CFL's are Accepted Simultaneously in Polynomial Time and Log Squared Space
*125/78	P.T. Cox and T. Pietrzykowski	Deduction Plans: a Basis for Intelligent Backtracking
*126/78	Lorna Stewart	A Class of Tree Representable Graphs
*127/78	Mario T. Hattori	A Survey of Finite-Difference Methods For Numerical Solution of Hyperbolic Partial Differential Equations
- * 128/78	Leo Gotlieb	Optimal Multi-Way Search Trees

* Not available - may be obtained at a charge through:
Interlibrary Loans Section
Science and Medicine Library
University of Toronto
Toronto, Canada M5S 1A5

TECHNICAL REPORT

(Continued)

Number	Author	Title
* 129/78	Kenneth R. Jackson	Variable Stepsize, Variable Order Integrand Approximation Methods for the Numerical Solution of Ordinary Differential Equations
130/79	Clifford A. Addison	Implementing A Stiff Method Based upon the Second Derivative Formulas
* 131/79	James F. Allen	A Plan-Based Approach to Speech Act Recognition
* 132/79	Martin Dowd	Propositional Representation of Arithmetic Proofs
* 133/79	A. Borodin S. Cook	A Time-Space Tradeoff for Sorting on a General Sequential Model of Computation
134/79	P. Keast	On the Null Spaces of Fully Symmetric Basic Rules for Quadrature Formulas in s-Dimensio
135/79	Y.S. Moon	On the Numerical Solution of the Definite Generalized Eigenvalue Problem
136/79	S. Ho-Tai, R.L. Johnston R. Mathon	Software for solving boundary value problems for Laplace's equation using fundamental solutions
137/80	Arnold L. Rosenberg	Issues in the Study of Data Encodings
138/80	Rakesh K. Agarwal	An Investigation of the Subgraph Isomorphism Problem
138/80	H. James Hoover	Some Topics in Circuit Complexity
* 139/80	Bryan M. Kramer	The Representation of Program in the Procedural Semantic Network Formalism

* Not available - may be obtained at a charge through:
Interlibrary Loans Section
Science and Medicine Library
University of Toronto
Toronto, Canada M5S 1A5

TECHNICAL REPORT

(Continued)

Number	Author	Title
140/80	Christopher B. Wilson	Relativization, Reducibilities, and the Exponential Hierarchy
141/80	Stephen A. Cook	Towards A Complexity Theory of Synchronous Parallel Computation
142/80	Charles Colbourn	The Complexity of Graph Isomorphism and Related Problems
143/80	A. Borodin	Structured vs General Models in Computational Complexity
144/80	R. Aleliunas/ A. Rosenberg	On Embedding Rectangular Grids in Square
145/80	Patrick Dymond	Simultaneous Resource Bounds and Parallel Computation
146/80	Marlene Colbourn	Cyclic Block Designs: Computational Aspects of Their Construction and Analysis
147/80	Clifford A. Addison	Numerical Methods for A Class of Second Order ODE's Arising in Structural Dynamics
148/81	J.C. Diaz, G. Fairweather and P. Keast	FORTRAN Packages for Solving Almost Block Diagonal Linear Systems by Modified Alternate Row and Column Elimination
149/81	Mohamed S. Kamel	Improving the Efficiency of Stiff ODE Solvers by Partitioning
150/81	P. Keast, G. Fairweather & J. Diaz	A Comparative Study of Finite Element Methods for the Solution of Second Order Linear Two-Point Boundary Value Problems
151/81	D. Cooperstock	Alternative Axiomatizations of Models of the Lambda-Calculus
152/81	Y. Yesha	On Certain Polynomial-Time Truth-Table Reducibilities of Complete Sets to Sparse Sets
153/81	W.T. Reeves and P. Sermer	Efficient Representation of Curves in Computer Graphics

* Not available - May be obtained at a charge through:
Interlibrary Loans Section
Science and Medicine Library
University of Toronto
Toronto, Ontario, Canada M5S 1A7

TECHNICAL REPORT

Number	Author	Title
154/81	P.M. Hanson & W.H. Enright	Controlling the Defect in Existing Variable-Order Adams Codes for Initial Value Problems
155/81	J. Von Zur Gathen	Hensel & Newton Methods in Valuation Rings
156/82	Borodin/Hopcroft/ Von zur Gathen	Fast Parallel Matrix and GCD Computations
157/82	Robert P. Duncan	A Runge-Kutta Method Using Variable Stepsizes for Volterra Integral Equations of the 2nd Kind
158/82	G. Fairweather & P. Keast	ROWCOL - A Package for Solving Block Diagonal Linear Systems arising in H^{-1}-Galerkin and collocation-H^{-1}-Galerkin Methods
159/82	Yaacov Yesha	Time-Space Tradeoffs for Matrix Multiplication and the Discrete Fourier Transform on any General Sequential Random-Access Compute
160/82	D. Corneil and M. Goldberg	A Non-Factorial Algorithm for Canonical Numbering of a Graph
161/82	Paul Beame	Random Routing in Constant Degree Networks
162/83	A. Borodin, S. Cook & N. Pippenger	Parallel Computation for Well-Endowed Rings and Space-Bounded Probabilistic Machines
163/83	J. Mark Keil	Decomposing Polygons into Simpler Components
164/83	Stephen A. Cook	The Classification of Problems which have Fast Parrallel Algorithms
165/83	Robin Dawes	Constructions of Minimally K-Connected Graphs
166/83	Romas Aleliunas	Probabilistic Parallel Communication
167/83	W.H. Enright & J.D. Pryce	Two Fortran Packages for Assessing Initial Value Methods

TECHNICAL REPORT

Number	Author	Title
168/83	Allan D. Jepson & Alastair Spence	The Numerical Solution of Nonlinear Equations Having Several Parameters.
169/83	Joseph G. Peters	Time-Accuracy Trade-Offs for Hard Miximization Problems
170/84	Tony F. Chan & Ken Jackson	The Use of Iterative Linear-Equation Solvers in Codes for Large Systems of Stiff IVPs for ODEs.
171/84	D.W. Decker & A. Jepson	Convergence Cones Near Bifurcation
172/84	Edward A. Severn	Maximal Partial Steiner Triple Systems
173/84	Pierre McKenzie	Parallel Complexity and Permutation Groups
174/84	Thomas Feather	The Parallel Complexity of Some Flow and Matching Problems
175/84	Paul Muir	Implicit Runge-Kutta Methods for Two-Point Boundary Value Problems
176/84	Kevin Burrage	The Order Properties of Implicit Multivalue Methods for Ordinary Differential Equations
177/84	Kevin Burrage	Order and Stability Properties of Explicit Multivalue Methods
178/85	Wayne Eberly	Very Fast Parallel Matrix and Polynomial Arithmetic
179/85	Christopher Wilson	Relativized Circuit Size and Depth
** 180/85	W.H. Enright K.R. Jackson S.P. Norsett and P.G. Thomsen	Interpolants for Runge-Kutta Formulas
181/85	Pierre McKenzie & Stephen A. Cook	The Parallel Complexity of Abelian Permutation Group Problems[1]

TECHNICAL REPORT

Number	Author	Title
182/85	Arvind Gupta	A Fast Parallel Algorithm for Recognition of Parenthesis Languages
183/85	J.M. Fine	Low Order Runge-Kutta-Nystrom Methods with Interpolants
184/85	Wendy Louise Seward	Defect and Local Error Control in Codes for Solving Stiff Initial-Value Problems
185/85	Lorna K. Stewart	Permutation Graph Structure and Algorithms
186/86	Anna Lubiw	Orderings and Some Combinatorial Optimization Problems with Geometric Applications
187/86	Raymond Reiter	A Theory of Diagnosis from First Principles.
188/86	J. von zur Gathen	Irreducible Polynomials over Finite Fields