IRREDUCIBLE TRINOMIALS OVER FINITE FIELDS

JOACHIM VON ZUR GATHEN

ABSTRACT. A necessary condition for irreducibility of a trinomial over a finite field, based on classical results of Stickelberger and Swan, is established. It is applied in the special case $\mathbb{F}_3$, and some experimental discoveries are reported.

Mathematics Subject Classification 2000: primary 11T06, secondary 12Y05, 68W30

1. INTRODUCTION

Trinomials are polynomials with three nonzero terms. Their computational advantages have frequently been pointed out. Ben-Or (1981) writes: *In order to make residue computation mod $g(x)$ easier one looks for special types of irreducible polynomials such as $g(x) = x^n+x+a$, $a \in \mathbb{Z}_p$.* In cryptography, Canteaut & Filiol (2001) attack some stream ciphers via the factorization of trinomials, and trinomials have been used as a highly efficient data structure for representing nonprime finite fields in exponentiation and discrete logarithm computations (Schroeppel *et al.* 1995, von zur Gathen & Nöcker 2002). Schroeppel *et al.* (1995) write: *The irreducible trinomial $T(u)$ has a structure that makes it a pleasant choice for representing the field*, and De Win *et al.* (1996): *The reduction operation can be speeded up even further if an irreducible* trinomial *is used.* Menezes *et al.* (1997), §5.4.2, say that *choosing an irreducible trinomial [...] can lead to a faster implementation of the field arithmetic.* They now form part of the IEEE Standard Specifications for Public-Key Cryptography: *The reduction of polynomials modulo $p(t)$ is particularly efficient if $p(t)$ has a small number of terms. [...] Thus, it is a common practice to choose a trinomial for the field polynomial, provided that one exists. If an irreducible trinomial of degree m does not exist, then the next best polynomials are the* pentanomials (IEEE (2000), A.3.4, p. 80).

Trinomials over finite fields also occur in other application areas. They are used for characterization and construction of almost perfect non-linear mappings (Carlet *et al.* (1998), Helleseth *et al.* (1999)) and of orthogonal arrays (Munemasa (1998)). They are related to words of weight 3 and the minimal distance of certain cyclic codes (Charpin *et al.* (1997), Charpin *et al.* (1999)) and yield linearly recurrent sequences with special properties (Goldstein & Zierler (1968), Golomb & Gong (1999)).

The bulk of this literature deals with $\mathbb{F}_2$ as the ground field, but Albert (1957) deals with general finite fields, and $\mathbb{F}_3$ occurs in Charpin *et al.* (1999) and Helleseth *et al.* (1999). Special trinomials arise in connection with the additive version of Hilbert's Theorem 90. As an example, $x^q - x - a \in \mathbb{F}_q[x]$ is irreducible for any $a \in \mathbb{F}_q^\times$, and if α is a root of it, then $x^q - x - a\alpha^{q-1}$ is irreducible in $\mathbb{F}_q(\alpha)[x]$; see Ore (1934) and Kaplansky (1972), Theorems 32 and 52. The degrees of the

Date: May 6, 2002.

irreducible factors of $x^{2q^m+1} + x^{q^m-1} + 1$ and of $x^{(q^m+1)/2} + ax + b$ in $\mathbb{F}_q[x]$ are studied in Carlitz (1970) and Estes & Kojima (1996), respectively.

The main results here give a necessary (but not sufficient) condition for irreducibility of trinomials over a finite field $\mathbb{F}_q$, and its application to $q = 3$ (Theorems 4 and 8). Somewhat to our surprise, the experiments in $\mathbb{F}_3[x]$ (see section 5) did not find any irreducible trinomial in some classes where the theory allows them.

A classical result of Stickelberger (1897) determines the parity of the number of irreducible factors of a squarefree polynomial in terms of the quadratic character of its discriminant. This was taken up by Dalen (1955), and Swan (1962) provides a simple formula for the discriminant of a trinomial. See also Golomb (1967), Chapter 5, and Berlekamp (1968), Section 6.6. Loidreau (2000) has applied this to trinomials $x^n \pm x^k \pm 1 \in \mathbb{F}_3[x]$ and found congruences for n and k which, together with the number of times that 2 divides n and k, characterize the property of being squarefree and having an odd number of irreducible factors. Any irreducible polynomial enjoys this property, but not vice versa.

Based on Swan's results, we show by a different approach that indeed the property depends only on the residues of n, k, n_1, and k_1 modulo certain numbers which are determined by the field size, where n_1 and k_1 are n and k, respectively, divided by $\gcd(n, k)$. Although these congruences characterize the stated property exactly, they give, of course, only a necessary condition for irreducibility. In fact, some of the congruence classes contain only reducible polynomials. Applying this to $\mathbb{F}_3$, we find a short list of small trinomials whose factorization is sufficient to completely characterize the property.

These factorizations take a few seconds on a workstation, once programmed. They even can, in principle, be checked by hand. However, the advantage of delegating the tedious checking of case by case to a machine is underlined by the fact that we found three corrections to Loidreau's handcrafted table.

The table plus three easy simplifications, namely reversal, the substitution of $-x$ for x, and the recognition of "systematic" linear factors, reduce the work for listing all irreducible trinomials of a given degree to about 8.2% of the number of test polynomials if we checked each trinomial.

For $2 \le n \le 1500$, we found irreducible trinomials for all but 220 values. For these exceptions, irreducible quadrinomials were found. It is conjectured that irreducible polynomials with at most four terms exist in $\mathbb{F}_q[x]$ for all degrees and all $q \ge 3$.

Some of our experimental findings defy explanation (by this author, at least). The probability p of being irreducible for uniformly random monic polynomials in $\mathbb{F}_3[x]$ of degree at most 1500 is about $1/1500$ (see below). But for a random trinomial, it is larger than $4p$, and over $6p$ in $\mathbb{F}_2[x]$. On the other hand, there are some congruence classes in which our theory allows irreducible polynomials, but where there are none (in the range of our experiments).

In characteristic 2, the property is nicely described by the results of Vishne (1997). It is interesting to note that a similar result holds over $\mathbb{Q}$ in a special case: Selmer (1956) shows that $x^n + x + 1$ is irreducible in $\mathbb{Q}[x]$ if and only if $n \not\equiv 2 \bmod 3$.

An Extended Abstract of this work has appeared in the Proceedings ACM ISSAC 2001, editor Bernard Mourrain, pp. 332–336.

2. Swan's condition

We fix the following notation.

(1) $n > k \geq 1$ are integers, q is a power of the odd prime p, $a, b \in \mathbb{F}_q^\times$, $f = x^n + ax^k + b \in \mathbb{F}_q[x]$, r is the number of irreducible factors of f in $\mathbb{F}_q[x]$, $D \in \mathbb{F}_q$ its discriminant, $d = \gcd(n,k)$, $n_1 = n/d$, and $k_1 = k/d$.

The following two results from Swan (1962) are fundamental for our question.

Fact 2 (Swan 1962). *In the above notation, we have the following for odd q.*

(i) *If f is squarefree, then $r \equiv n \bmod 2$ if and only if D is a square in $\mathbb{F}_q$,*

(ii) $D = (-1)^{n(n-1)/2} \cdot b^{k-1} \cdot (n^{n_1} b^{n_1-k_1} - (-1)^{n_1}(n-k)^{n_1-k_1} k^{k_1} a^{n_1})^d$.

As Swan mentions, (i) goes back to Stickelberger (1897). It provides a necessary condition for irreducibility, and is, in fact, originally due to Pellet (1878). Dickson (1906) proves this fact, apparently without being aware of the previous work.

On our way to studying irreducibility, the following more general "Stickelberger" property of $f \in \mathbb{F}_q[x]$ is of central interest:

(S) f is squarefree and has an odd number of irreducible factors.

Corollary 3. *In the above notation, we have for odd q*

$$f \text{ has property (S)} \iff D^{(q-1)/2} = (-1)^{n+1}.$$

Proof. It is well-known that f is squarefree if and only if $D \neq 0$. Now we assume that $D \neq 0$. Then D is a square if and only if $D^{(q-1)/2} = 1$, and

$$r \text{ odd} \iff (n \text{ is odd and } D^{(q-1)/2} = 1) \text{ or } (n \text{ is even and } D^{(q-1)/2} = -1). \quad \square$$

We denote by $\nu_\ell(m)$ the multiplicity of a prime ℓ in any nonzero integer m. The following is the main result of this paper.

Theorem 4. *Let q be a power of the odd prime p, $f = x^n + ax^k + b$ with $a, b \in \mathbb{F}_q^\times$, $n > k \geq 1$, $d = \gcd(n,k)$, $n_1 = n/d$, $k_1 = k/d$, $m_2 = p \cdot (q-1)$, and $m_1 = lcm(4, m_2)$. Then the discriminant of f and property (S) depend only on the following residues:*

$$n \bmod m_1,\ k \bmod m_2,\ n_1 \text{ and } k_1 \bmod q-1.$$

Proof. We let $D = \mathrm{disc}(f) \in \mathbb{F}_q$. Also, we let n^*, k^* be two further integers with $n^* > k^* \geq 1$, r^* be the number of irreducible factors of $x^{n^*} + ax^{k^*} + b$ in $\mathbb{F}_q[x]$, D^* its discriminant and d^*, n_1^*, and k_1^* analogous to the quantities defined above. We suppose furthermore that $n \equiv n^* \bmod m_1$, $k \equiv k^* \bmod m_2, n_1 \equiv n_1^* \bmod (q-1)$, and $k_1 \equiv k_1^* \bmod (q-1)$. The claim of the theorem is that $D = D^*$ and, if $D \neq 0$, that $r \equiv r^* \bmod 2$.

By Fermat's Little Theorem, we have $c^u = c^v$ for any $c \in \mathbb{F}_q$ and positive integers u, v with $u \equiv v \bmod q-1$. It follows that the first two factors in Fact 2(ii) for D equal those in D^*. Furthermore, $n \equiv n^* \bmod p$ and $k \equiv k^* \bmod p$, and all the exponents in the third factor in D equal modulo $q-1$ their analogues in D^*. (We note that all these exponents are positive integers.) It is now sufficient to show that $d \equiv d^* \bmod q-1$; then $D = D^*$, and Fact 2 (i) implies the second claim.

Let ℓ be a prime divisor of $q-1$, and $\lambda = \nu_\ell(q-1)$, $\mu = \nu_\ell(d)$, $\mu^* = \nu_\ell(d^*)$. If $\mu \geq \lambda$, then $n^* \equiv n \equiv 0 \bmod \ell^\lambda$ and $k^* \equiv k \equiv 0 \bmod \ell^\lambda$ imply that $\mu^* \geq \lambda$. Now we suppose that $\mu < \lambda$. Then μ equals at least one of $\nu_\ell(n)$ and $\nu_\ell(k)$. We assume that $\mu = \nu_\ell(n)$; the other case is analogous. Now $n_1 = n/d$ is a unit modulo ℓ^λ, and so is $n_1^* \equiv n_1 \bmod \ell^\lambda$. Thus we have

$$d = \frac{n}{n_1} \equiv \frac{n^*}{n_1^*} = d^* \bmod \ell^\lambda.$$

Since this holds for any prime power divisor ℓ^λ of $q-1$, we conclude that $d \equiv d^* \bmod q-1$. □

Our assumptions imply that the actual value of D is fixed, while it would be sufficient to fix its quadratic character. But we do not see an interesting way of weakening the assumptions accordingly.

In the case $p = 2$, one may assume (using reversion, as below) that exactly one of n and k is even. Then in the last factor of Swan's formula for D, one of the two summands vanishes. This simplifies things considerably, and Vishne (1997) has given a complete characterization of trinomials with property (S) in this case. Cazacu & Simovici (1973) deal with roots of special trinomials in characteristic 2.

3. Two symmetries

Let $s, k_0 = 0 < k_1 < \cdots < k_{s-1} = n$ be nonnegative integers, and

$$S = \Big\{ \sum_{0 \leq i < s} a_i x^{k_i} : \text{ all } a_i \in \mathbb{F}_q^\times, a_n = 1 \Big\} \subseteq \mathbb{F}_q[x]$$

be the set of monic polynomials with support $\{k_0, \ldots, k_{s-1}\}$. Each $f \in S$ is s-sparse, and its *monic reversal* $\tilde{f} = a_0^{-1} x^n f(x^{-1}) = a_0^{-1} \sum_{0 \leq i < s} a_i x^{n-k_i}$ is also s-sparse. Squarefreeness and the number of irreducible factors are preserved under this transformation.

For $u \in \mathbb{F}_q^\times$ and $f \in S$, we set $f_u = u^{-n} f(ux)$. Then $f_u \in S$, and $u \mapsto (f \mapsto f_u)$ is a group action of $\mathbb{F}_q^\times$ on S. Again, this preserves squarefreeness and the number of irreducible factors.

Theorem 5. *In the above notation, let $g = \gcd(q-1, k_1, \ldots, k_{s-1})$. Then each orbit of the action of $\mathbb{F}_q^\times$ has size $(q-1)/g$.*

Proof. We let $z \in \mathbb{F}_q^\times$ be a primitive element of the multiplicative group, $f \in S$, and $j \in \mathbb{N}$. Then we have

$$\begin{aligned}
f = f_{z^j} &\iff \sum_{0 \leq i < s} a_i x^{k_i} = z^{-jn} \sum_{0 \leq i < s} a_i (z^j x)^{k_i} \\
&\iff 1 = z^{-jn} z^{jk_i} = (z^j)^{k_i - n} \text{ for all } i < s \\
&\iff \operatorname{ord}(z^j) \mid n - k_i \text{ for all } i < s \\
&\iff \operatorname{ord}(z^j) \mid k_i \text{ for all } i < s \\
&\iff \frac{q-1}{\gcd(j, q-1)} = \operatorname{ord}(z^j) \mid \gcd(q-1, k_1, \ldots, k_{s-1}) = g \\
&\iff \frac{q-1}{g} \mid \gcd(j, q-1) \iff \frac{q-1}{g} \mid j.
\end{aligned}$$

The last condition does not depend on f.

It follows that the kernel of the action is generated by $z^{(q-1)/g}$ and has g elements. Therefore each orbit has precisely $(q-1)/g$ elements. □

As indicated below, several types of polynomials have property (S) but do not contain irreducible polynomials, because each member has a root in $\mathbb{F}_q$. We might hope to rule out further types by finding roots in extensions of $\mathbb{F}_q$. But the following result shows that this does not work.

Lemma 6. *Let q be a power of the prime p, $f \in \mathbb{F}_q[x]$, β in some algebraic extension of $\mathbb{F}_q$, and $\beta \neq 0$.*

(i) *Let k_0 and m be nonnegative integers with $m \geq 1$ and $f(\beta) + \beta^{k_0+im} = 0$ for all $i \geq 0$, and $m' = m/p^{\nu_p(m)}$. Then $\beta^{m'} = 1$.*

(ii) *If furthermore $m = m_2 = p(q-1)$ as in Theorem 4, then $\beta \in \mathbb{F}_q$.*

Proof. (i) It is sufficient to take $i = 0$ and $i = 1$, subtract the two equations and factor out β^{k_0} to obtain $\beta^m = 1$. If e is the degree of $\mathbb{F}_q(\beta)$ over $\mathbb{F}_p$ and $j = \lceil \nu_p(m)/e \rceil$, then by Fermat's Little Theorem in $\mathbb{F}_q(\beta)$

$$\beta^{m'} = (\beta^{m'})^{p^{ej}} = \beta^{m \cdot p^{ej} - \nu_p(m)} = 1.$$

(ii) The first part implies that $\beta^{q-1} = 1$. □

4. The special case $\mathbb{F}_3$

The search for irreducible trinomials in $\mathbb{F}_3[x]$ was the starting point for this work. This may be considered a worthwhile goal in itself. The special motivation for us is that irreducible trinomials furnish a representation of non-prime finite fields which is particularly efficient for exponentiation, which in turn is the primary operation in several cryptosystems; see von zur Gathen & Nöcker (1997), Gao *et al.* (2000), von zur Gathen & Nöcker (2002). In the last paper, $\sigma_q(n)$ is defined as the minimal number of terms in irreducible polynomials of degree n in $\mathbb{F}_q[x]$, and it is conjectured that for all $n \geq 1$, $\sigma_2(n) \leq 5$, and $\sigma_q(n) \leq 4$ for $q \geq 3$. The conjecture has been verified for $q = 2$ and $n < 10\,000$; see Golomb (1967), chapter 5, Zierler & Brillhart (1969), Zierler (1970), Fredricksen & Wisniewski (1981), von zur Gathen & Nöcker (2002). The experiments reported in this paper show its truth for $q = 3$ and $n \leq 1500$.

We set

$$s = (n_1 \bmod 2, k_1 \bmod 2), \text{ where } n_1 = n/\gcd(n,k), k_1 = k/\gcd(n,k). \tag{7}$$

Using a concise notation, s can take the three values $11, 10$, and 01, since n_1 and k_1 are not both even.

Theorem 8. *Let $f = x^n \pm x^k \pm 1 \in \mathbb{F}_3[x]$ be a trinomial.*

(i) *f has property (S) if and only if the value of $k \bmod 6$ appears in Table 1, in column f and row $n \bmod 12$, possibly with a condition on s.*

(ii) *If f is irreducible, then the value of $k \bmod 6$ appears non-italicized in Table 1.*

Proof. We have $12 \cdot 6 \cdot 3 = 216$ values of (n,k,s) to consider for each form of f. Some simplifications are possible. We assume that $n \equiv n^* \bmod 12$ and $k \equiv k^* \bmod 6$. If n is odd, then $\nu_2(n) = \nu_2(n^*) = 0$, and $\nu_2(k) > 0$ if and only if $\nu_2(k^*) > 0$.

$n \bmod 12$	$x^n + x^k + 1$	$x^n + x^k - 1$	$x^n - x^k + 1$	$x^n - x^k - 1$
0	—	$2, 4$	—	$2, 4$
1	*0, 1, 3, 4*	$0, 1, 3, 4$	$0, 1, 3, 4$	$0, 1, 3, 4$
2	*0, 2, 3, 5*	1	$0, 2, 3, 4, 5$	1
3	*4, 5*	$2, 5$	$1, 2$	$1, 4$
4	—	$0, 1, 3, 4, (2; 01, 10)$	—	$0, 1, 3, 4, (2; 01, 11)$
5	—	4	$1, 4$	1
6	*1, 2, 4, 5*	$1, 5$	*1*, $2, 4$, *5*	$1, 5$
7	—	2	$2, 5$	5
8	—	$0, 2, 3, 5, (4; 01, 10)$	—	$0, 2, 3, 5, (4; 01, 11)$
9	*1, 2*	*1*, 4	$4, 5$	*2*, 5
10	*0, 1, 3, 4*	5	0, *1*, 2, *3*, 4	5
11	*0, 2, 3, 5*	$0, 2$, *3*, *5*	$0, 2, 3, 5$	*0*, *2*, $3, 5$

TABLE 1. The values of $k \bmod 6$ for which the polynomial in $\mathbb{F}_3[x]$ at the column head with $1 \le k < n$ has property (S). The entry $(2; 01, 10)$ means that $k \equiv 2 \bmod 6$ and $s = 01$ or $s = 10$ are possible. Values in italics correspond to reducible polynomials.

Thus $s = s^*$. Similarly, if k is odd, then $s = s^*$. In these 54 cases, there is only one relevant value of s. If $n \equiv 2 \bmod 4$ and k is even, then $\nu_2(n) = 1$ and $\nu_2(k)$, $\nu_2(k^*) \ge 1$, so that $s, s^* \in \{11, 10\}$. In these 9 cases, there are two values of s, and in the remaining nine cases, three values of s. The total comes to $54 \cdot 1 + 9 \cdot 2 + 9 \cdot 3 = 99$ possibilities for (n, k, s). Then we factor $99 \cdot 4$ polynomials, one for each case, on a computer algebra system. (Each of them takes only seconds on a workstation.) The value is entered into Table 1 if and only if the test polynomial has property (S). Finally, we put those values in italics where the polynomial has 1 or -1 as a root, namely the whole column $x^n + x^k + 1$ with 24 entries, and 18 further cases with the factor $x - 1$.

Now for an arbitrary trinomial $f = x^n \pm x^k \pm 1$ over $\mathbb{F}_3$, Theorem 4 guarantees that our test polynomial for $(n \bmod 12, k \bmod 6, s)$ has property (S) if and only if f has it, and then the corresponding value appears in the table. □

It is no surprise that Table 1 is invariant under monic reversal and the operation of $\mathbb{F}_3^\times$, that is, the negation of x. Each column is also invariant under the substitution of (n, k) by $(-n, -k) \bmod (12, 6)$; this is easy to explain.

Proposition 9. *Assume the notation (1), m_1 and m_2 as in Theorem 4, and furthermore $1 \le k^* < n^*$ with $n^* \equiv -n \bmod m_1$, $k^* \equiv -k \bmod m_2$, $n_1^* \equiv -n_1 \bmod (q-1)$, $k_1^* \equiv -k_1 \bmod (q-1)$, and $f^* = x^{n^*} + a x^{k^*} + b$. Then f has property (S) if and only if f^* does.*

Proof. We use the notation (1) also for the starred values. It is sufficient to show that if f has property (S), then so does f^*. So we assume (S) for f; in particular, $D \ne 0$. By Fact 2, it suffices to see that $D^* = D$. We denote by

$$u = n^{n_1} b^{n_1 - k_1} \text{ and } v = (-1)^{n_1} (n-k)^{n_1 - k_1} k^{k_1} a^{n_1}$$

the two summands in the last factor of Fact 2 (ii), and similarly for the starred quantities. As in the proof of Theorem 4, we find $d \equiv d^* \bmod (q-1)$. Fermat's

Little Theorem now implies that

$$u^* = (-n)^{n_1^*} b^{n_1^* - k_1^*} = (-1)^{n_1} n^{n_1} b^{n_1 - k_1} = (-1)^{n_1} u,$$

and similarly $v^* = (-1)^{n_1} v$. Thus

$$\frac{D^*}{D} = (-1)^n \left(\frac{u^* - v^*}{u - v}\right)^d = (-1)^n \left((-1)^{n_1}\right)^d = 1. \qquad \square$$

Loidreau (2000) took Swan's result over $\mathbb{F}_3$ and worked out, for general n and k, the necessary case distinctions. He found that the property under consideration depends only on n mod 12 and k mod 6. We turned this around, and first proved the latter result, then ran an experiment for each case. In order to compare with Loidreau's results, we first note that $\nu_2(n) > \nu_2(k)$ corresponds to $s = 01$, $\nu_2(n) = \nu_2(k)$ to $s = 11$, and $\nu_2(n) < \nu_2(k)$ to $s = 10$. We find that our table agrees with his results, except that for $x^n - x^k + 1$ his values $(3, 4)$ and $(3, 5)$ for (n mod 12, k mod 6) should not be included, and that $(7, 2)$ is missing.

Is ours an "elegant" proof? Well, Theorem 8 refers to a messy table and therefore cannot be considered elegant. Seiden (2001) writes: *In the best of circumstances, the computational method allows us to give the inelegant part of a proof, at which we would turn our noses up, to a computer for verification.* In some sense, we may have achieved this goal, by proving Theorem 4 and leaving the messy calculations to a computer.

5. Experiments

We computed all irreducible trinomials in $\mathbb{F}_3[x]$ of degrees $n \le 1500$, and found some for each $n \ge 2$ except for 220 values of n. Some statistics are given in Figure 1. It is no surprise that the residue classes of n mod 12 with sparse rows in Table 1 are

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\#n$	6	10	14	9	17	18	17	15	17	17	18	15	20	12	14

n mod 12	0	1	2	3	4	5	6	7	8	9	10	11
$\#n$	27	12	7	34	7	34	5	31	12	33	12	6
$\#k$	4	8	5	4	$9\frac{2}{3}$	4	6	4	$9\frac{2}{3}$	4	5	8

Figure 1. The number $\#n$ of n with $\sigma_3(n) = 4$ and $100i \le n < 100(i+1)$ (top) and in each congruence class modulo 12 (bottom). The last row $\#k$ gives the number of non-italicized values of k in each row of 1.

represented frequently. For each "exceptional" n, we found an irreducible quadrinomial.

Ree (1971) proves that for any n, the number of irreducible trinomials $x^n + x + a \in \mathbb{F}_p[x]$ with $a \in \mathbb{F}_p^\times$ tends to p/n for large p. Just like general polynomials, these special trinomials are irreducible with probability about $1/n$. Can we expect something similar for general trinomials over $\mathbb{F}_3$ and growing n? Is irreducibility equidistributed except for the constraints imposed by Theorem 8? The answer is: no; there seem to be conditions that do not follow from the present theory. It is also quite unexpected that the probability to be irreducible is over four times as high for trinomials than for general polynomials, in our experimental range.

$x^n + x^k - 1$						
$n \backslash k$	0	1	2	3	4	5
0			145,0,0$_r$		145,0,0$_r$	
1	161$_{r-}$				149$_{r-}$	
2		137$_{r-}$				
3			188$_{r-}$			
4	231,0,0$_r$	251$_{r-}$	121,0,0$_r$	251$_{r-}$	231,0,0$_r$	
5					158$_{r-}$	
6		158$_{r-}$				158$_{r-}$
7			160$_{r-}$			
8	229,0,0$_r$		229,0,0$_r$	241$_{r-}$	106,0,0$_r$	241$_{r-}$
9					170$_{r-}$	
10						108$_{r-}$
11	143$_{r-}$		179$_{r-}$			

$x^n - x^k + 1$						
$n \backslash k$	0	1	2	3	4	5
0						
1	$-_{(1,0,\pm)}$	$r-_{(1,0,\pm)}$		$r-_{(1,4,\pm)}$	$-_{(1,4,\pm)}$	
2	84,76$_r$		$r_{(2,0,\mp)}$		81,81	
3		$r-_{(3,2,\pm)}$	$-_{(3,2,\pm)}$			
4						
5		$r-_{(5,4,\pm)}$			$-_{(5,4,\pm)}$	
6			72,97$_r$		$r_{(6,2,\mp)}$	
7			$-_{(7,2,\pm)}$			$r-_{(7,2,\pm)}$
8						
9					$-_{(9,4,\pm)}$	$r-_{(9,4,\pm)}$
10	79,87$_r$		75,75		$r_{(10,0,\mp)}$	
11	$-_{(11,0,\pm)}$		$-_{(11,2,\pm)}$	$r-_{(11,2,\pm)}$		$r-_{(11,0,\pm)}$

FIGURE 2. Irreducible trinomials in $\mathbb{F}_3[x]$ with degree $n \le 1500$.

Figure 2 counts the irreducible trinomials. A table entry is indexed by

$$e = (n_0, k_0, s_0, a, b) \tag{10}$$

with row index $0 \le n_0 < 12$, column index $0 \le k_0 < 6$, $s_0 \in \{01, 10, 11\}$ and $a, b \in \{\pm 1\}$.

We have condensed the table by applying the symmetries of Section 3. It turned out that only $(a, b) = (1, -1)$ (top table) and $(a, b) = (-1, 1)$ (bottom table) have to be considered. The subscript r means that monic reversal yields another entry with the same numerical value, and the subscript $r-$ corresponds to three other entries obtained by monic reversal and the negation of x. The values of s are ordered as 01, 10, 11, and the values of k mod 6 are split into six columns $0, \ldots, 5$. Thus the first entry 145,0,0$_r$ means that we found 145 irreducible trinomials $x^n + x^k - 1$ with $n \equiv 0 \bmod 12$, $k \equiv 2 \bmod 6$, and $s = 01$, so that $e = (0, 2, 01, 1, -1)$, and none for $s = 10$ or $s = 11$. The subscript r points to another entry given by monic reversal and not shown in the table, namely 145,0,0 for $x^n - x^k - 1$ with $n \equiv 0 \bmod 12$ and $k \equiv 4 \bmod 6$. Similarly, the entry 161$_{r-}$ says that 161 irreducible polynomials were found for $e = (1, 0, 10, 1, -1)$, and the subscript $r-$ points to the other three entries

$(1,1,11,-1,-1)$, $(1,0,10,-1,1)$, and $(1,1,11,-1,1)$ obtained by monic reversal, by substituting $-x$, and by applying both symmetries, respectively. For each of these three entries, we also have 161 irreducible trinomials.

In the bottom table of Figure 2, the first entry $-_{(1,0,\pm)}$ means that we have 161 irreducible trinomials for $e = (1,0,10,-1,1)$, just as for $(1,0,10,1,-1)$ obtained by negating x. The entry $r_{(2,0,\mp)}$ in the row $n = 2$ points to the $(84,76)$ irreducible trinomials $x^n - x^k + 1$ for $n \equiv 2$, $k \equiv 0$, and $s = (10,11)$. The condensation makes the tables somewhat shorter; for example, all $x^n - x^k - 1$ are obtained from some $x^n + x^{k'} - 1$ by symmetry. Furthermore, necessarily duplicated values are eliminated and "accidentally" duplicated values (see below) are clearly visible. The two tables together correspond to the two middle columns in Table 1. Because of the condition $1 \le k < n$, entries corresponding to each other according to Proposition 9 are not necessarily equal, but have reasonably close values.

All entries are such that Theorem 8 allows them to be positive. Thus the 16 entries equal to zero (actually corresponding to 32 entries) came as a big surprise. For $n \le 1500$ they say that

$$\begin{aligned} &n \equiv 0 \bmod 4,\ k \equiv 2 \bmod 6,\ x^n + ax^k + b \text{ irreducible} \\ &\qquad \Longrightarrow s = 01 \text{ (that is, } \nu_2(n) > \nu_2(k)). \end{aligned} \tag{11}$$

We have no explanation for this phenomenon. We also observe several repeated values in Figure 2; namely,

$$n \equiv 0 \bmod 4 \Longrightarrow \begin{array}{l} \text{the entries for } (n,k,s,a,b) \\ \text{and } (n,(n-k) \operatorname{rem} 6,s,a,b) \text{ are equal.} \end{array} \tag{12}$$

Again, we do not know whether this is a coincidence.

Open Question 13. *Are (11) or (12) true in general?*

We also observed that trinomials are over four times as likely to be irreducible than general polynomials, in the range of our experiments. If $I_q(n)$ denotes the number of irreducible monic polynomials $f \in \mathbb{F}_q[x]$ of degree n, then

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot q^d \approx \frac{q^n}{n},$$

and the probability for a random monic f of degree at most N to be irreducible is

$$\begin{aligned} p_q(N) &= \frac{\sum_{1 \le n \le N} I_q(n)}{\sum_{0 \le n \le N} q^n} = \frac{q-1}{q^{N+1}-1} \sum_{\substack{1 \le n \le N \\ d|n}} \frac{1}{n} \mu\left(\frac{n}{d}\right) \cdot q^d \\ &= \frac{q-1}{q-q^{-N}} \sum_{\substack{k \le N \\ m = \lfloor N/k \rfloor}} \frac{1}{k} \mu(k) \cdot q^{-N+m} s_q(m), \end{aligned}$$

where $s_q(m) = \sum_{1 \le d \le m} q^{d-m}/d$. We have $s_q(m) = q^{-1} s_q(m-1) + m^{-1}$ for $m \ge 2$, $m^{-1} \le s_q(m) \le 1$, and for large N

$$p_q(N) \approx \left(1 - \frac{1}{q}\right) s_q(N).$$

We find

$$p_3(1500) \approx 0.00066 \approx 1/1499.5.$$

On the other hand, there are $4 \cdot \sum_{2 \le n \le N} (n-1) = 2N(N-1)$ monic trinomials in $\mathbb{F}_3[x]$ of degree at most N, and 12 498 monic irreducible trinomials of degree at most 1500, so that in this range a trinomial has a chance of

$$r = \frac{12\,498}{2 \cdot 1500 \cdot 1499} \approx 0.00278 \approx 1/359.82$$

to be irreducible. We have

$$r/p_3(1500) \approx 4.16739.$$

Thus a random trinomial is over four times as likely to be irreducible than a random polynomial, in this range.

For $q = 2$, we have

$$p_2(1500) \approx 0.00067 \approx 1/1499, \; r = \frac{4575}{1\,124\,250} \approx 0.004, \; r/p_2(1500) \approx 6.1,$$

with r as above for $\mathbb{F}_2$ instead of $\mathbb{F}_3$. Hence for polynomials of degree up to 1500 in $\mathbb{F}_2[x]$, trinomials are more than six times as likely to be irreducible as general ones.

Open Question 14. *What happens in general?*

For an $e = (n_0, k_0, s_0, a, b)$ and $n \equiv n_0 \bmod 12$, the set of all trinomials corresponding to e is

$$S_n(e) = \{x^n + ax^k + b \in \mathbb{F}_3[x] \colon k \equiv k_0 \bmod 6, s = s_0\},$$

with s as in (7), and the number of irreducible ones is

$$t_n(e) = \#\{f \in S_n(e) \colon f \text{ irreducible}\}.$$

Theorem 8 says that $t_n(e) = 0$ unless e appears non-italicized in Table 1. Is irreducibility evenly distributed among these e?

For $N \in \mathbb{N}$ and an entry e as in (10), we set

$$T_N(e) \;=\; p_3(N)^{-1} \sum_{\substack{2 \le n \le N \\ n \equiv n_0 \bmod 12}} t_n(e) \;/ \sum_{\substack{2 \le n \le N \\ n \equiv n_0 \bmod 12}} \#S_n(e),$$

so that trinomials in $S_n(e)$ are irreducible with probability $p_3(N) \cdot T_N(e)$, averaged over $n \le N$. Figure 3 gives the relevant values of $T_{1500}(e)$. The missing values are given by the pointers in Figure 2, or else are zero. For every $n_0 < 12$, there is some e as in (10) so that the proportion of irreducible polynomials in $T_n(e)$ is at least fifteen times as high as in the set of all polynomials, within our experimental range.

Of the $288 = 12 \cdot 6 \cdot 4$ possible values of (n, k, f) for Table 1, only 114 appear, 4 of them with a restriction on s. These restrictions occur in four cases, where $n \equiv 4 \bmod 12$ and $k \equiv 2 \bmod 6$, or $n \equiv 8 \bmod 12$ and $k \equiv 4 \bmod 6$. In Theorem 15, we will show the following statistics for these restrictions. If we fix such an n and consider all such k with $1 \le k < n$, then $s = 11$ and $s = 10$ occur equally often, and $s = 01$ about four times as often as each of the other two values. Thus the four restrictions on s rule out about $1/6$ in each case, for a total of about $2/3$. Thus we are left with about $113\frac{1}{3}$ cases.

Removing those with 1 or -1 as a root leaves only $71\frac{1}{3}$ candidates. Lemma 6 says that we do not have to look for other systematic factors. Now monic reversal makes about half of the candidates superfluous, since we may restrict to $k \le n/2$.

	$x^n + x^k - 1$						$x^n - x^k + 1$		
$n\backslash k$	0	1	2	3	4	5	0	2	4
0			20.7,0,0		20.7,0,0				
1	15.6				14.4				
2		13.1					16.3,14.7		15.7,15.7
3			18.0						
4	33.5,0,0	24.1	17.4,0,0	24.1	33.5,0,0				
5					15.2				
6		15.2				15.2		13.9,18.5	
7			15.4						
8	32.7,0,0		32.7,0,0	23.1	15.3,0,0	23.1			
9					16.3				
10						10.4	15.3,16.6	14.3,14.3	
11	13.7		17.0						

FIGURE 3. The relevant values of $T_{1500}(e)$.

The action of $\mathbb{F}_3^\times$ has orbits of size $2/\gcd(2,k,n)$, and it is sufficient to consider only one representative from each orbit. The size is 2 unless both k and n are even, when it is 1. The former occurs in 48 non-italicized entries, the latter in $23\frac{1}{3}$ entries. Thus on average we have a reduction by a factor of $47\frac{1}{3}/71\frac{1}{3} = 71/107 \approx 66.4\%$. The total number of candidate trinomials will be close to

$$71\frac{1}{3} \cdot \frac{1}{2} \cdot \frac{71}{107} = 23\frac{2}{3}$$

out of the 288 possibilities, a reduction to about 8.2%.

We next determine the gain that results from ruling out one of the possibilities $s = 11$ or $s = 10$ in four entries of Table 1. For $i \in \{01, 10, 11\}$, we denote by $t_i(n)$ the number of integers k with $1 \le k < n$, $k \equiv 2 \bmod 6$, and $(n_1 \bmod 2, k_1 \bmod 2) = i$. For $N \in \mathbb{N}$, we let

$$T(N) = \sum_{\substack{4 \le n \le N \\ n \equiv 4 \bmod 12}} t(n), \qquad T_{11}(N) = \sum_{\substack{4 \le n \le N \\ n \equiv 4 \bmod 12}} t_{11}(n).$$

The first part of the next theorem shows that $t_{10}(n) = t_{11}(n)$, and the ratio $t(n)/t_{11}(n)$ is about $2^{\nu_2(n)}$ (if $2^{\nu_2(n)} \ll n$). Its second part shows that this ratio is close to 6 on average. Thus the proportion $t_{01} : t_{10} : t_{11}$ is about $4 : 1 : 1$, on average.

Theorem 15. *(i) Let n be a positive integer with $n \equiv 4 \bmod 12$, and $e = \nu_2(n)$. Then*

$$t_{10}(n) = t_{11}(n) = \frac{n - (-2)^e}{6 \cdot 2^e}.$$

(ii) The ratio $T(N)/T_{11}(N)$ tends to 6, and more precisely

$$6\left(1 - \frac{42}{N} + O(\frac{\log N}{N^2})\right) \le \frac{T(N)}{T_{11}(N)} \le 6\left(1 + \frac{52}{N} + O(\frac{\log N}{N^2})\right).$$

The proof is omitted. For $76 \le N \le 4000$, the values of $N \cdot (T(N)/T_{11}(N) - 6)$ are between -60 and 20. The corresponding results also hold in the other case of interest, where $n \equiv 8 \bmod 12$ and $k \equiv 4 \bmod 6$.

A heuristic estimate goes as follows. For a randomly chosen monic polynomial of degree n in $\mathbb{F}_q[x]$, the probability of it being irreducible is about $1/n$. If we choose

nt many independently, then the probability that none is irreducible is about

$$\left(1 - \frac{1}{n}\right)^{nt} \approx e^{-t}.$$

There are roughly $n(q-1)^2$ monic trinomials of degree n in $\mathbb{F}_q[x]$, and if irreducibility occurred about as often as for random polynomials (which it does not), we would find $e^{-(q-1)^2}$ for the "probability" that $\sigma_q(n) \geq 4$. (Of course, $\sigma_q(n)$ is a well-defined integer, with no random choices involved.) The value $e^{-2^2} \approx 1.8\%$ is much smaller than the rate of almost 15% we found for $n \leq 1500$, and shows that this heuristic is not worth much.

Not even slightly discouraged by this, we also apply the heuristics to quadrinomials, and find the following upper bound for the "probability" that $\sigma_q(n) \geq 5$ for some n:

$$\sum_{n \geq 3} (1 - \frac{1}{n})^{n^2(q-1)^3/2} \approx \sum_{n \geq 3} e^{-n(q-1)^3/2} \approx e^{-3(q-1)^3/2}.$$

The last number evaluates to about $0.6 \cdot 10^{-5}$ for $q = 3$.

Acknowledgements

The author thanks Olaf Müller for substantial help with the computations and the preparation of the tables, and an anonymous referee for helpful suggestions and the reference to Pellet's paper.

References

A. A. Albert (1957). On certain trinomial equations in finite fields. *Annals of Mathematics* **66**(1), 170–178.

M. Ben-Or (1981). Probabilistic algorithms in finite fields. In *Proceedings of the 22nd Annual IEEE Symposium on Foundations of Computer Science,* Nashville TN, 394–398.

Elwin R. Berlekamp (1968). *Algebraic Coding Theory.* McGraw-Hill, New York.

Anne Canteaut & Eric Filiol (2001). Ciphertext only reconstruction of stream ciphers based on combination generators. In *Proceedings of Fast Software Encryption (FSE 2000),* B. Schneier, editor, number 1978 in Lecture Notes in Computer Science. Springer-Verlag, New York. URL `http://link.springer.de/link/service/series/0558/bibs/1978/19780165.htm`.

Claude Carlet, Pascale Charpin & Victor Zinoviev (1998). Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems. *Designs, Codes and Cryptography* **15**, 125–156.

L. Carlitz (1970). Factorization of a special polynomial over a finite field. *Pacific Journal of Mathematics* **32**(3), 603–614.

C. Cazacu & D. Simovici (1973). A New Approach of Some Problems Concerning Polynomials Over Finite Fields. *Information and Control* **22**, 503–511.

P. Charpin, A. Tietäväinen & Victor Zinoviev (1997). On binary cyclic codes with minimum distance $d = 3$. *Problems of Information Transmission* **33**(4), 287–296.

Pascale Charpin, Aimo Tietäväinen & Victor Zinoviev (1999). On the Minimum Distances of Non-Binary Cyclic Codes. *Designs, Codes and Cryptography* **17**, 81–85.

Kåre Dalen (1955). On a theorem of Stickelberger. *Mathematica Scandinavica* **3**, 124–126.

ERIK DE WIN, ANTOON BOSSELAERS, SERVAAS VANDENBERGHE, PETER DE GERSEM & JOOS VANDEWALLE (1996). A Fast Software Implementation for Arithmetic Operations in $GF(2^n)$. In *Advances in Cryptology: Proceedings of ASIACRYPT 1996,* Kyongju, Korea, KWANGJO KIM, editor, number 1163 in Lecture Notes in Computer Science, 65–76. Springer-Verlag. ISSN 0302-9743. URL `ftp://ftp.esat.kuleuven.ac.be/pub/cosic/dewin/asia96p103.ps.gz`.

L. E. DICKSON (1906). Criteria for the irreducibility of functions in a finite field. *Bulletin of the American Mathematical Society* **13**(1), 1–8.

DENNIS R. ESTES & TETSURO KOJIMA (1996). Irreducible Quadratic Factors of $x^{(q^n+1)/2} + ax + b$ over $\mathbb{F}_q$. *Finite Fields and Their Applications* **2**(2), 204–213. ISSN 1071-5797.

H. FREDRICKSEN & R. WISNIEWSKI (1981). On Trinomials $x^n + x^2 + 1$ and $x^{8l\pm3} + x^k + 1$ Irreducible over $GF(2)$. *Information and Control* **50**, 58–63.

SHUHONG GAO, JOACHIM VON ZUR GATHEN, DANIEL PANARIO & VICTOR SHOUP (2000). Algorithms for Exponentiation in Finite Fields. *Journal of Symbolic Computation* **29**(6), 879–889. URL `http://www.idealibrary.com/servlet/doi/10.1006/jsco.1999.0309`.

JOACHIM VON ZUR GATHEN & MICHAEL NÖCKER (1997). Exponentiation in Finite Fields: Theory and Practice. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: AAECC-12,* Toulouse, France, TEO MORA & HAROLD MATTSON, editors, number 1255 in Lecture Notes in Computer Science, 88–113. Springer-Verlag. ISSN 0302-9743.

JOACHIM VON ZUR GATHEN & MICHAEL NÖCKER (2002). Exponentiation using addition chains for finite fields. In preparation.

RICHARD M. GOLDSTEIN & NEAL ZIERLER (1968). On Trinomial Recurrences. *IEEE Transactions on Information Theory* **IT-14**(1), 150–151.

SOLOMON W. GOLOMB (1967). *Shift Register Sequences.* Holden-Day Series in Information Systems. Holden-Day, Inc., San Francisco, California. With portions co-authored by Lloyd R. Welch, Richard M. Goldstein, and Alfred W. Hales.

SOLOMON W. GOLOMB & GUANG GONG (1999). Periodic Binary Sequences with the "Trinomial Property". *IEEE Transactions on Information Theory* **45**(4), 1276–1279.

TOR HELLESETH, CHUNMING RONG & DANIEL SANDBERG (1999). New Families of Almost Perfect Nonlinear Power Mappings. *IEEE Transactions on Information Theory* **45**(2), 475–485.

IEEE (2000). IEEE Standard Specifications for Public-Key Cryptography. Technical Report IEEE Std 1363-2000, Institute of Electrical and Electronics Engineers, Inc., 3 Park Avenue, New York, NY 10016-5997, USA.

I. KAPLANSKY (1972). *Fields and Rings.* University of Chicago Press, Chicago.

PIERRE LOIDREAU (2000). On the Factorization of Trinomials over $\mathbb{F}_3$. Technical Report 3918, Institut national de recherche en informatique et en automatique (INRIA). URL `http://www.inria.fr/RRRT/RR-3918.html`.

ALFRED J. MENEZES, PAUL C. VAN OORSCHOT & SCOTT A. VANSTONE (1997). *Handbook of Applied Cryptography.* CRC Press, Boca Raton FL.

AKIHIRO MUNEMASA (1998). Orthogonal Arrays, Primitive Trinomials, and Shift-Register Sequences. *Finite Fields and Their Applications* **4**(3), 252–260.

OYSTEIN ORE (1934). Contributions to the theory of finite fields. *Transactions of the American Mathematical Society* **36**, 243–274.

A.-E. PELLET (1878). Sur la décomposition d'une fonction entière en facteurs irréductibles suivant un module premier p. *Comptes Rendus de l'Académie des Sciences Paris* **86**, 1071–1072.

RIMHAK REE (1971). Proof of a Conjecture of S. Chowla. *Journal of Number Theory* **3**, 210–212.

RICHARD SCHROEPPEL, HILARIE ORMAN, SEAN O'MALLEY & OLIVER SPATSCHECK (1995). Fast Key Exchange with Elliptic Curve Systems. In *Advances in Cryptology: Proceedings of CRYPTO '95,* Santa Barbara CA, DON COPPERSMITH, editor, number 963 in Lecture Notes in Computer Science, 43–56. Springer. ISSN 0302-9743. URL

http://theory.lcs.mit.edu/ dmjones/hbp/crypto/crypto95.html.
Steve Seiden (2001). Can a Computer Proof be Elegant? *SIGACT News* **60**(1), 111–114.
Ernst S. Selmer (1956). On the irreducibility of certain trinomials. *Mathematica Scandinavica* **4**, 287–302.
L. Stickelberger (1897). Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper. *Verhandlungen des ersten Internationalen Mathematiker-Kongresses, Zürich,* 182–193.
Richard G. Swan (1962). Factorization of polynomials over finite fields. *Pacific Journal of Mathematics* **12**, 1099–1106.
Uzi Vishne (1997). Factorization of Trinomials over Galois Fields of Characteristic 2. *Finite Fields and Their Applications* **3**(4), 370–377.
Neal Zierler (1970). On $x^n + x + 1$ over $GF(2)$. *Information and Control* **16**, 502–505.
Neal Zierler & John Brillhart (1969). On Primitive Trinomials (Mod 2), II. *Information and Control* **14**, 566–569.

Fachbereich Mathematik & Informatik, Universität Paderborn, D-33095 Paderborn, Germany

E-mail address: gathen@upb.de