RECOGNISING ELEMENTS OF FINITE FIELDS

RICHARD G.E. PINCH

Abstract. In this note we describe two algorithms for calculating the expressions which find the roots of one irreducible polynomial over a finite field in terms of the roots of another such polynomial.

1. Introduction

It is well known that there is precisely one finite field up to isomorphism of every prime power order $q = p^n$. Every such field may be realised as the field generated over $\mathbb{F}_p$ by a root of an irreducible polynomial, $f(X)$, say, of degree n. Hence, given two such polynomials $f(X)$ and $g(Y)$ of the same degree, each of the roots of f must be expressible as a polynomial, of degree at most n, in any root of g, and conversely.

In this note we describe two algorithms for calculating the expressions which find the roots of one irreducible polynomial over a finite field in terms of the roots of another such polynomial.

Each method makes use of a suitable group Γ defined by algebraic operations over $L = \mathbb{F}_p$. We find an element γ of small order r defined over the field $K = \mathbb{F}_{p^n}$, and represent γ both as a polynomial $\alpha(x)$ in a root x of f and similarly as a polynomial $\beta(y)$ in a root y of g. We must choose r so that the element γ generates K, rather than any subfield, over $\mathbb{F}_p$. The two representations of the same element γ are then used to find a representation of x as a polynomial in y.

In the first, *cyclotomic*, method the group Γ is just the multiplicative group K^* of the field K. Unfortunately, if the order of this group is divisible only by "large" factors, then there will be many elements of order r in Γ and the time taken to compare all the possible elements of order r will also be large. We may view this drawback of the cyclotomic method as analogous to the corresponding disadvantage of Pollard's $p - 1$ factorisation algorithm: see, for example, Koblitz [1]. Pursuing this analogy, we describe a second, *elliptic*, method which proceeds by taking Γ to be the group of points on a suitably chosen elliptic curve defined over K. Since there are about $4\sqrt{p}$ elliptic curves defined over $\mathbb{F}_p$ we have better chance of finding a small order r to work with.

In each case the method will apply to any pair of irreducible polynomials over L once the appropriate Γ and r have been chosen.

If we regard one of the two representations of K as "standard" then the problem is equivalent to solving a polynomial equation over K. Further references are given, for example, in Lidl and Niederreiter [3] and Lenstra [2].

Date: 6 April 2006.

1.1. **Cyclotomic method.** As an example of the cyclotomic method, consider the irreducible polynomials $f(X) = X^{23} + 8X^2 + X + 9$ and $g(Y) = Y^{23} + 3Y^2 + 4Y + 9$ of degree 23 over $L = \mathbb{F}_{11}$. We take Γ to be the multiplicative group of $K = \mathbb{F}_{11^{23}}$. Then Γ has order 895430243255237372246530 and this is divisible by $r = 829$. We verify that 829 does not divide the order of the multiplicative group of any subfield of K (in fact the only such subfield of K in this case is $\mathbb{F}_{11}$ itself) and so an element of order 829 in K^* must be a field generator of K over $\mathbb{F}_{11}$. Taking the element x and raising it to the power $895430243255237372246530/829 = 1080132983420069206570$ we find that

$$\begin{aligned}\alpha(x) &= 7 + 8x + 4x^2 + 4x^4 + 4x^5 + 10x^6 + 4x^7 + 3x^8 + 5x^9 \\ &\quad +2x^{10} + 6x^{11} + 4x^{12} + 8x^{13} + 6x^{14} + 4x^{15} + 4x^{16} \\ &\quad +5x^{17} + 7x^{18} + 4x^{19} + x^{20} + 8x^{22}\end{aligned}$$

and similarly from y we obtain

$$\begin{aligned}\beta(y) &= 1 + y + 4y^2 + 4y^3 + 9y^4 + y^5 + 6y^6 + 3y^7 + 3y^8 + 3y^9 \\ &\quad +6y^{10} + 5y^{11} + 6y^{12} + 8y^{13} + y^{14} + 9y^{15} + 4y^{16} \\ &\quad +3y^{17} + 5y^{18} + y^{19} + 10y^{20} + 10y^{21} + 6y^{22}\end{aligned}$$

are elements of order 829 in their respective fields.

We note that, since the multiplicative group of a field is cyclic, there is a probability of $\frac{1}{829}$ that an element γ chosen at random is already an 829^{th} power. In this case the corresponding value of $\alpha(x)$, say, would turn out to be 1. In general we see that the expected number of trials required to find an element of exact order r would be $\frac{r}{r-1}$.

We know that the fields $K_1 = L[X]/(f)$ and $K_2 = L[Y]/(g)$ must be isomorphic. Let ϕ denote such an isomorphism: then ϕ is determined by the image of x, say $\phi(x) = \sum_0^{n-1} \phi_i y^i$. The element $\phi(\alpha)$ in K_2 corresponding to α in K_1 must be a power of β, say $\phi(\alpha) = \beta^s$ for some $s \le r$, since the multiplicative group of a field is cyclic.

We proceed by trying each possible value of s in turn until we find ϕ. Substituting for $\phi(x)$ in the equation $\phi(\alpha) = \beta^s$ gives a set of simultaneous linear equations in the ϕ_i. We solve these and obtain a map $\phi^{(s)}$. We test this by evaluating the minimal polynomial $g(Y)$ on the candidate $\phi^{(s)}(x)$. If the result is zero then $\phi^{(s)}$ is indeed an isomorphism of fields and the problem is solved.

In the example we find that α corresponds to β^{14} and that the isomorphism is given by

$$\begin{aligned}\phi(x) &= 8 + 9y + y^2 + 2y^3 + 7y^4 + 4y^5 + 6y^6 + 10y^7 + 9y^8 \\ &\quad +10y^9 + 2y^{10} + 2y^{12} + 10y^{13} + 2y^{14} + 7y^{15} + y^{16} \\ &\quad +3y^{17} + 2y^{18} + 2y^{20} + y^{21} + y^{22}.\end{aligned}$$

1.2. **Elliptic method.** Unfortunately the cyclotomic method is not always practical. For example, in the case of the field of degree 11 over $\mathbb{F}_5$, the multiplicative group ${\mathbb{F}_{5^{11}}}^*$ has order $48828124 = 4.12207031$ and 12207031 is prime. We could still find easily find $\alpha(x)$, $\beta(y)$ but there is an impractically large number of values of s to try to solve the equation $\phi(\alpha) = \beta^s$: in fact, we are reduced to trying all possible linear maps between the vector spaces to see which of them is a field isomorphism.

We therefore consider taking Γ to be the points on an elliptic curve E defined over $\mathbb{F}_5$. The points on such a curve defined over L form an abelian group under the addition law defined by the "tangent–chord" process: we refer to Koblitz [1] for an

introduction to elliptic curves and to Silverman [5] for details. We need to be able to compute the order of Γ, that is, the number of points on E defined over $\mathbb{F}_{5^{11}}$.

In general the number of points on an elliptic curve E defined over $L = \mathbb{F}_p$ is $p + 1 - t$ where t can take any value satisfying $\mod |t| < 2\sqrt{p}$: this inequality is equivalent to saying that the equation $X^2 - tX + p$ has complex conjugates roots τ and $\bar{\tau}$. The number of points on E which are defined over an extension $K = \mathbb{F}_{p^n}$ is then given by $(1-\tau^n)(1-\bar{\tau}^n)$. For a given curve E over L, we can now compute the number of points over K by a simple recurrence relation (and in particular much faster than counting!)

For the case $K = \mathbb{F}_{5^{11}}$ we choose the elliptic curve E with equation $Y^2 = X^3 + 4X + 3$ over $L = \mathbb{F}_5$. We find that E has 3 points defined over L, the number of points on E over $\mathbb{F}_{5^{11}}$ is $48841719 = 23.2123553$, and the coordinates of a point on E of order 23 must generate this field over L. Furthermore, since 23 does not divide 2123553, the group Γ is again cyclic.

As an application of the elliptic method in this case, consider the irreducible polynomials $f(X) = X^{11} + 3X + 3$ and $g(Y) = Y^{11} + Y^5 + 4Y^3 + 4Y + 2$ over $L = \mathbb{F}_5$, and let E^*d denote the curve $dY^2 = X^3 + 4X + 3$, the "twist" of E by d. If d is a square in K then E^*d is isomorphic to E over K and in particular has the same number of points defined over K. If we $(x, y; z)$ denote the point $\left(\frac{x}{z^2}, \frac{y}{z^3}\right)$ on E^*d, so that the identity for the group law, the point at infinity on the y-axis, is $(0, 1; 0)$, then the point $P = (x, 1; 1)$ lies on E^*d where $d = x^3 + 4x + 3$ and d is a square in $L[X]/(f)$. Accordingly if we let $A = 2123553.P$ then

$$\begin{aligned} A \;=\; & (3x + 2x^2 + 4x^4 + x^6 + x^7 + x^8 + 2x^9 + 3x^{10}, \\ & 3 + 3x^2 + 4x^3 + x^4 + 4x^5 + x^7 + 4x^8 + 3x^9 + 4x^{10}; \\ & 3x + x^2 + x^3 + 4x^4 + 4x^5 + 2x^7 + 2x^8 + 4x^9 + 3x^{10}) \end{aligned}$$

is a point of order $r = 23$ on $E^*(x^3 + 4x + 3)$. Similarly, we consider the point $Q = (3 + y, 1; 1)$ on $E^*(2 + y + 4y^2 + y^3)$ and take $B = 2123553.Q$, so

$$\begin{aligned} B \;=\; & (3 + 3y + y^2 + 2y^3 + 2y^4 + y^5 + 2y^6 + 2y^7 + 4y^8 + 3y^9 + 3y^{10}, \\ & 3 + y + y^2 + 2y^3 + 4y^4 + 2y^5 + 4y^7 + y^9 + 4y^{10}; \\ & 4 + 4y + 2y^2 + 3y^3 + 3y^4 + 3y^6 + 2y^8 + y^9 + y^{10}) \end{aligned}$$

is of order 23. We therefore consider the equation $\phi(A) = s.B$, finding the map $\phi^{(s)}$ by applying the same technique as for the cyclotomic method to the x-coordinates of the points, and find that $\phi^{(s)}$ is a field isomorphism in the case $s = 1$, with

$$\phi(x) = 4y + y^3 + 4y^4 + 2y^5 + 3y^6 + 3y^7 + y^8 + 2y^9 + 3y^{10}.$$

1.3. **Remarks.** Both the cyclotomic and elliptic methods rely on finding a point of small order r on the associated group Γ, but once r and Γ have been chosen for a given pair (p, n) then the method can be applied for any pair of irreducible polynomials.

If we consider the fields of degree up to 100 over $\mathbb{F}_5$, and assume that we are willing to consider points of order up to 10000, then there are 30 possible degrees (the smallest being 11) for which the cyclotomic method is not applicable, and for the extension of degree 80 we need to consider points of order $r = 25601$. However, one of the two methods will work for every degree up to 100, the largest value of r in the elliptic method being 4405, again for degree 80.

In most cases the elliptic curve method provides a significantly smaller value of r. This is not always the case, as the case of degree 9 shows. Here the two methods would each require $r = 19$ and computing in the cyclotomic group is approximately 15 times faster than in the elliptic group for the same value of r.

We give a full description of the two methods, together with tables for the groups and orders required for extensions of degree at most 100 over $\mathbb{F}_p$ for $p \leq 97$ in Matthews, Parker and Pinch (1991).

References

[1] Neal Koblitz, *A course in number theory and cryptography*, Graduate Texts in Mathematics, vol. 114, Springer–Verlag, New York, 1987.
[2] Hendrik W. Lenstra jr, *Algorithms for finite fields*, [4], 76–85.
[3] Rudolf Lidl and Harald Niederreiter, *Finite fields*, Encyclopaedia of Mathematics and its applications, vol. 20, Addison–Wesley, Reading Mass., 1983, Republished, Cambridge University Press, 1984.
[4] J.H. Loxton (ed.), *Number theory and cryptography*, LMS Lecture notes, vol. 154, Cambridge University Press, 1990.
[5] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer–Verlag, Berlin, 1986.

2 Eldon Road, Cheltenham, Glos GL52 6TU, U.K.
E-mail address: rgep@chalcedon.demon.co.uk