The World's Most Interesting Class of Integral Polynomials

Rudolf Lidl and Gary L. Mullen

Dedicated to Professor David Elliott on the Occasion of his 70th birthday

1 Introduction

What is the world's most interesting class of integral polynomials, i.e. what is the world's most interesting set of polynomials, one of each degree, that have integer coefficients? Some people might say $\{x^n\}$; well this class is a little boring. Can we do better? Write down your favorite class $\{f_n(x)\}$ of integral polynomials and let's see how they stack up for interesting properties against the following.

Our favorite class begins as follows. Let a be an integer and define

$$\begin{aligned} D_0(x,a) &= 2 \\ D_1(x,a) &= x \\ D_2(x,a) &= x^2 - 2a \\ D_3(x,a) &= x^3 - 3ax \\ D_4(x,a) &= x^4 - 4ax^2 + 2a^2 \\ D_5(x,a) &= x^5 - 5ax^3 + 5a^2x \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

In general we have the following recurrence

$$D_n(x,a) = xD_{n-1}(x,a) - aD_{n-2}(x,a), \qquad n \geq 2$$

where the two initial polynomials are $D_0(x,a) = 2$ and $D_1(x,a) = x$.

There are several ways of viewing our polynomials and as an exercise, we ask that you derive each.

As a closed form we have

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i},$$

JCMCC 37 (2001), pp. 87-100

where $\lfloor n/2 \rfloor$ denotes the largest integer $\leq n/2$. A second closed form is given by

$$D_n(x,a) = (\frac{x+\sqrt{x^2-4a}}{2})^n + (\frac{x-\sqrt{x^2-4a}}{2})^n.$$

There is a functional equation so that if x can be written as $x = u + a/u$ for some u, then

$$D_n(x,a) = u^n + \frac{a^n}{u^n}.$$

We also have the generating function

$$\sum_{n=0}^{\infty} D_n(x,a)z^n = \frac{2-xz}{1-xz+az^2}.$$

The polynomials satisfy second order differential equations which correspond to the well known differential equations for the Chebyshev polynomials. In particular, the polynomial $D_n(x,a)$ satisfies the differential equation

$$(x^2-4a)y'' + xy' - n^2y = 0.$$

For those of you with more classical tastes, we point out that our polynomials $D_n(x,a)$ are not unrelated to a well studied class of polynomials. Consider the classical Chebyshev polynomials $T_n(x)$ defined for each integer $n \geq 0$ by $T_n(x) = \cos\,(n \arccos x)$. Working for the moment over the complex numbers, let $u = e^{i\alpha}$ so that $x = u + 1/u = 2\cos\alpha$. Then, as is easily checked,

$$D_n(x,1) = u^n + u^{-n} = e^{in\alpha} + e^{-in\alpha} = 2\cos(n\alpha) = 2T_n(\cos\alpha) = 2T_n(x/2).$$

Hence our polynomials are related to the classical Chebyshev polynomials, and in fact some authors use the latter terminology.

L.E. Dickson was the first to seriously study various algebraic and number theoretic properties of these polynomials. In particular, he studied these polynomials as part of his Ph.D. thesis at the University of Chicago in 1896; see also Dickson [7]. In 1923 I. Schur [23] suggested that these polynomials be named in honor of Dickson and so we will continue with this convention to call the polynomials $D_n(x,a)$ Dickson polynomials as was the case in [16].

2 Solvability by radicals

In teaching courses on abstract algebra, it is of interest to have classes of polynomials that can be solved by radicals. Unfortunately it is not easy to find concrete examples of such polynomials for each degree $n \geq 1$ other than minor variations of x^n for which it is possible to explicitly write down the solution in terms of radicals. Dickson polynomials however come to the rescue.

Consider the polynomial equation $D_{2n+1}(x, a) = b$. Then

$$x = (\frac{b + \sqrt{b^2 - 4a^{2n+1}}}{2})^{\frac{1}{2n+1}} + (\frac{b - \sqrt{b^2 - 4a^{2n+1}}}{2})^{\frac{1}{2n+1}}. \qquad (1)$$

is a solution. Check! Such a derivation was first obtained by Dickson [7] and later in [25] Williams provided the following proof. Since every mathematical paper ought to have at least one proof, we will include the argument by Williams as follows.

Let x be a root and consider $\lambda^2 - x\lambda + a = (\lambda - \alpha)(\lambda - \beta) = 0$ so that $x = \alpha + \beta, a = \alpha\beta$. Hence $1 - x\lambda + a\lambda^2 = (1 - \alpha\lambda)(1 - \beta\lambda)$. We then have

$$\log(1 - x\lambda + a\lambda^2) = \log(1 - \alpha\lambda) + \log(1 - \beta\lambda)$$

$$= -\sum_{m=1}^{\infty} \frac{\alpha^m \lambda^m}{m} - \sum_{m=1}^{\infty} \frac{\beta^m \lambda^m}{m} = -\sum_{m=1}^{\infty} \frac{(\alpha^m + \beta^m)}{m} \lambda^m.$$

Since $\log(1 - x\lambda + a\lambda^2) = \log(1 - \lambda(x - a\lambda))$, the above becomes

$$-\sum_{m=1}^{\infty} \sum_{s=0}^{\lfloor m/2 \rfloor} \frac{(-1)^s}{m-s} \binom{m-s}{s} a^s x^{m-2s} \lambda^m.$$

Equating coefficients of λ we have

$$\frac{\alpha^m + \beta^m}{m} = \sum_{s=0}^{\lfloor m/2 \rfloor} \frac{1}{m-s} \binom{m-s}{s} (-a)^s x^{m-2s}.$$

Let $m = 2n+1$ so that $\alpha^{2n+1} + \beta^{2n+1} = D_{2n+1}(x, a)$. Thus the quadratic equation $y^2 - D_{2n+1}(x, a)y + a^{2n+1} = y^2 - by + a^{2n+1} = 0$ has roots α^{2n+1} and β^{2n+1}. On the other hand by the quadratic formula

$$y = \frac{b \pm \sqrt{b^2 - 4a^{2n+1}}}{2}$$

and hence

$$\alpha^{2n+1} = \frac{b + \sqrt{b^2 - 4a^{2n+1}}}{2}, \beta^{2n+1} = \frac{b - \sqrt{b^2 - 4a^{2n+1}}}{2}.$$

Finally since x is a root of the equation $D_{2n+1}(x, a) - b = 0$ and $x = \alpha + \beta$, we have the complete solution of our original equation.

Actually Dickson used this method to show that if $(2n+1, p^2-1) = 1$, then $D_{2n+1}(x, a)$ induces a permutation on the finite field F_p where p is a prime so that on substitution of the elements of F_p for x, we obtain all of the elements of F_p. We note from the solution (1) that if $(2n+1, p^2-1) = 1$, then in the field F_{p^2} one can take $(2n+1)$-roots in the field. Certainly one can then also take square roots as every element in F_p has a square root in the quadratic extension field F_{p^2}.

3 Permutations

Let p be an odd prime and consider reducing an integral polynomial $f(x)$ modulo p, i.e. reduce the integer coefficients modulo the prime p so that we may now view f as a function $f : F_p \rightarrow F_p$, where F_p denotes the field of integers modulo the prime p.

For which primes p and what values of a does $D_n(x, a)$ induce a permutation of the p elements in the field F_p? Could we be so lucky that a single condition works for all values of a? Unfortunately we aren't quite that lucky but if $a = 0$, our problem is easy since $D_n(x, 0) = x^n$ is a permutation if and only if $(n, p-1) = 1$. Why is this the case? Recall that the set F_p^* of nonzero elements of F_p forms a cyclic group under multiplication of order $p-1$. The rest of the argument is easy.

Now what about the general Dickson polynomial $D_n(x, a)$ where $a \neq 0$? We note from the functional equation that if $x = u + a/u$, then $u^2 - xu + a = 0$. This is a quadratic equation which will always have a solution in the quadratic extension field F_{p^2} of F_p. Moreover, x will be the sum of the roots of the equation and a will be the product.

Could it be since we are working in the quadratic extension field F_{p^2}, that $(n, p^2-1) = 1$ is the right condition to ensure that for $a \neq 0, D_n(x, a)$ permutes F_p? If only mathematics was always so easy to make the right conjecture! You prove using the functional equation that for $a \neq 0 \in F_p$, indeed $D_n(x, a)$ permutes the field F_p if and only if $(n, p^2-1) = 1$.

Cohen [5] shows that if p is a large prime compared to the degree of f, then the permutation polynomial f essentially comes from a Dickson polynomial; i.e. $f(x) = f_2(f_1(x))$ where f_2 is a monic polynomial and $f_1(x) = D_{m_1}(x^{m_2}, a) + \alpha$ with $a \neq 0$ and $\alpha \in F_p$; see [5] or [16] page 167.

Mathematicians are often greedy and not quite satisfied with conditions for single primes. Therefore we ask: could it be that $D_n(x, a)$ permutes F_p for many different primes p? A finite number? An infinite number? You can no doubt very quickly convince yourself that a given polynomial $D_n(x, a)$ can permute a number of fields F_p so let's not waste our time; let's see if we can decide whether it might permute infinitely many such prime fields F_p.

Let's first look at the slightly simpler case of the polynomial $D_n(x,0) = x^n$. Remember that in order for x^n to induce a permutation on the field F_p, n must satisfy $(n, p-1) = 1$. Thus what we need is to see whether we can round up infinitely many such primes p with $(n, p-1) = 1$. How do we proceed?

Fortunately there is an old theorem of Dirichlet from 1837 that will do the trick for us. Dirichlet's theorem says that if $(a,b) = 1$, then the sequence $ak + b$ of integers contains infinitely many primes p as k runs through the positive integers; see Apostol [1], page 146. Now back to our polynomial x^n, assume that n is odd, (if n is even $x^n = (-x)^n$), i.e. that $(n,2) = 1$. Now by Dirichlet's theorem, the sequence $nk + 2$ contains infinitely many primes p. Note that for each such prime p, we have $(n, p-1) = (n, nk+1)$ and if some prime say r, divided both n and $p-1$, it would thus have to divide 1, a contradiction! Thus for each of these infinitely many primes p from Dirichlet's theorem, we have $(n, p-1) = 1$ and hence for each of these infinitely many primes p we have that $D_n(x,0) = x^n$ induces a permutation on the field F_p.

Ok, does something similar work for the Dickson polynomial $D_n(x,a)$ where $a \neq 0$? And if so, how does it work? Convince yourself that if $(n,6) = 1$, then $D_n(x,a)$ induces a permutation on F_p for infinitely many primes p.

Now that you are feeling pretty good about how to find integral polynomials that permute F_p for infinitely many primes p, we ask if there are others? Sure there are, simply take some linear polynomial like $ax+b$ where a, b are integers with $a \neq 0$. Then clearly $ax+b$ will permute any field F_p as long as p doesn't divide a,-and since a only has a finite number of divisors, then we are in business: $ax + b$ will permute infinitely many prime fields F_p.

Can you construct others? In 1923 Schur conjectured in [23] that the answer is essentially, no; He conjectured that if $f \in Z[x]$ (when considered modulo p) is a permutation of F_p for infinitely many primes p, then f must be a composition of binomials $ax^n + b$ and Dickson polynomials. The first proof of this conjecture was given by Fried [10] in 1970 using considerable mathematical machinery including Riemann surfaces. Quite recently in [24] Turnwald gave an elementary (without complex analysis) but still not easy proof of this result. There is no truly easy proof known.

One might note that in the above cases, when considering polynomials of degree n, we needed the conditions $(n,2) = 1$ for x^n and $(n,6) = 1$ for $D_n(x,a)$ with $a \neq 0$ to permute F_p for infinitely many primes p. Does anything of interest arise when one considers $(n,30) = (n, 2\cdot 3\cdot 5) = 1$ and $(n, 2\cdot3\cdot5\cdot7) = 1$ etc.? Mullen showed in [19] that using such conditions one can get a matrix analogue of Schur's conjecture. In particular let $m \geq 2$ be a fixed integer. If $f \in Z[x]$ induces a permutation on the ring $F_p^{m\times m}$

of all $m \times m$ matrices over F_p for infinitely many primes p, then f is a composition of linear polynomials $\alpha_i x + \beta_i \in Q[x]$ and Dickson polynomials $D_{n_j}(x, a_j)$ with $a_j \neq 0 \in Z$ where every n_j is either an odd prime with $(n, 2\prod_{i=1}^{m}(2^{2i}-1)) = 1$ or a prime l dividing $\prod_{i=1}^{m}(2^{2i}-1)$ with $l > 2m+1$. In the above Q denotes the field of rational numbers.

We refer to Parshall [20] for a discussion of various other work of Dickson related to permutations (which Dickson called *substitution quantics* of degree n) as well as a summary of his work related to linear groups.

4 Value sets

Given a polynomial f over F_p, i.e. with coefficients in F_p, we define the *value set* V_f of f by $V_f = \{f(a) | a \in F_p\}$. Recalling that a polynomial of degree n over any field can have at most n roots, and noting that there are p distinct elements in F_p, we clearly have

$$\lfloor \frac{p-1}{n} \rfloor + 1 \leq |V_f| \leq p.$$

Hence a polynomial whose value set achieves the value p induces a permutation and those which achieve the above lower bound are called *minimal value set* polynomials, see Mills [18]. As noted in Gomez-Calderon and Madden [12], polynomials of degree n with value sets of small cardinality (less than twice the minimum) come from Dickson polynomials.

If one considers a polynomial f over F_p and asks for the cardinality $|V_f|$ of the value set V_f of f, it is in general a very difficult problem to determine $|V_f|$. For example if $f(x) = x^5 + x^3 + 5x^2 - 3x + 15$ is viewed as a polynomial over F_{17}, can you quickly determine $|V_f|$? What is $|V_{f_n}|$ for your favorite class $\{f_n(x)\}$ of polynomials?

In fact there are very few classes of polynomials for which the cardinality of the value set is known. The reader should check that over F_p

$$|V_{x^n}| = \frac{p-1}{\delta} + 1, \delta = (n, p-1) = 1.$$

As for Dickson polynomials $D_n(x, a)$ over F_p with $a \neq 0$, should we expect an analogous formula? Sure, since by now we have noticed that whenever something happens for x^n, something analogous usually happens for the corresponding general Dickson polynomial of the same degree. The polynomials $D_n(x, a)$ are indeed interesting and, in fact, we have from [4] that for $a \neq 0 \in F_p$

$$|V_{D_n(x,a)}| = \frac{p-1}{2(n, p-1)} + \frac{p+1}{2(n, p+1)} + \alpha,$$

where $\alpha = 0$, or $1/2$, or 1. In fact as indicated in [4], usually $\alpha = 0$.

5 Commutativity properties

What about various commuting properties? Of course our polynomials commute, as do polynomials from any class, under polynomial addition and multiplication. What about functional composition; i.e. is $f(g(x)) = g(f(x))$ for any two polynomials in our class? When are our polynomials closed under functional composition? Well certainly the class $\{x^n\}$ of power polynomials is closed under composition since $(x^n)^m = x^{nm} = x^{mn} = (x^m)^n$.

Here we must concede ground, although grudgingly, as not all Dickson polynomials with integral coefficients are closed under composition. However as indicated in [16] page 13, over an integral domain and hence in particular over the integers, they are closed under composition if and only if $a = 0$ or $a = 1$.

If a class (called a *permutable chain*) of integral polynomials (one of each degree > 1) commutes under composition, i.e. if any two integral polynomials in the class commute under functional composition, then this class must come essentially from only two classes (This result actually also holds over any integral domain.). You guessed that one of the classes is the class $\{x^n\}$ and from the above, we suspect you might guess that the other class must be the class $\{D_n(x, 1)\}$, see page 13 of [16] for details.

By the way, how is your favorite class $\{f_n(x)\}$ of polynomials faring? How many of the above properties do they share? If you are yet to be convinced that our polynomials are more interesting than yours, let's continue our efforts at convincing you.

6 Irreducible polynomials

In many applications of algebra, in particular in algebraic coding theory for the error-free transmission of information and in cryptology for the secure transmission of information, one often needs to construct a field F_{p^n} of dimension n over F_p; i.e. we need an irreducible of degree n over a prime field F_p. While we know, see for example Lidl and Niederreiter [17] page 93, that for each integer $n \geq 2$ and any prime p there is an irreducible of degree n over F_p, it is not an easy problem to construct such an irreducible.

Here again Dickson polynomials come to the rescue, at least for some degrees. For example in [11] the following is shown. Let $n \geq 3$ be odd and let $a, b \in F_p$ with $a \neq 0$. Let $x^2 + bx + a^n = (x - \beta_1)(x - \beta_2)$ where the multiplicative order of β_i is e_i. Then $D_n(x, a) + b$ is irreducible over F_p if and only if each prime factor of n divides e_i but not $(p^2 - 1)/e_i$. Ok, this is a little technical, can we use it for example to get irreducibles of infinitely many degrees n over the field F_p where p is odd? You bet we can! As a corollary of the above, if ρ is a *primitive element* (recall this means that ρ multiplicatively generates the group F_p^* of all nonzero elements of F_p), then the polynomial $D_n(x,1)-(\rho+\rho^{-1})$ is irreducible of degree n over F_p for all

$$n = r_1^{k_1}\cdots r_t^{k_t},$$

where $r_1,\ldots,r_t$ are distinct odd prime factors of $p-1$, and $k_1 \geq 0,\ldots,k_t \geq 0$ are nonnegative integers.

7 Bases

The finite field F_{p^n} may be viewed as a vector space over the base field F_p and in this way, it is a vector space of dimension n over F_p. A particularly useful basis to have handy is a *normal* basis; an element $\alpha \in F_{p^n}$ generates a normal basis if the elements

$$\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$$

form a basis. Thus these elements must be independent and they must span the field F_{p^n} over F_p. Eisenstein [9] conjectured the normal basis theorem for finite fields; and Hensel [13] was the first of many authors to give proofs of this important fact that every extension field has a normal basis over the base field.

Why is a normal basis useful and important for finite field calculations? The reason is as follows. In doing calculations in the field F_{p^n} one oftens needs to take p-th powers β^p of an element β. If

$$\beta = a_0\alpha + a_1\alpha^p + \cdots + a_{n-1}\alpha^{p^{n-1}},$$

then

$$\beta^p = a_{n-1}\alpha + a_0\alpha^p + \cdots + a_{n-2}\alpha^{p^{n-1}},$$

since for any γ in the field $F_{p^n}, \gamma^{p^n} = \gamma$. Thus taking a p-th power β^p of an element β simply reduces to a cyclic shift of the vector representing the coefficients of β in the normal basis.

In 1987 Lenstra and Schoof [15] proved the primitive normal basis theorem; namely that every extension field has an element α which not only generates a normal basis of F_{p^n} over F_p, but that element α may be taken to be a primitive element of F_{p^n}.

Recall that the field F_{p^n} has a subfield of order p^d if and only if d divides n. Since we are greedy, might there be an element $\alpha \in F_{p^n}$ which simultaneously generates a normal basis over both F_{p^d} as well as over the base field F_p? Being even greedier, might there be an α in F_{p^n} which simultaneously generates a normal basis over F_{p^d} for all d dividing n, i.e. α simultaneously generates a normal basis over all intermediate subfields? With a difficult and technical argument, Blessenohl and Johnsen [2] showed that this is indeed the case. Such elements α are said to be *completely normal.*

Surely you must be thinking that Dickson polynomials can't possibly play a role in this rather complicated computational setting. Wrong! For a polynomial $f(x)$ of degree n, define the reciprocal polynomial $f^*(x)$ by $f^*(x) = x^n f(1/x)$ so that $f^*(x)$ is also of degree n and note that if $f(x)$ is irreducible or primitive, then so is the reciprocal polynomial $f^*(x)$. In [22] Scheerhorn proved that if $n \geq 3$ is odd and $a, b \in F_p$ with $D_n(x,a) - b$ irreducible over F_p, then the polynomial $(D_n(x,a) - b)^*$ is completely normal over F_p. Here by completely normal polynomial we simply mean a polynomial whose roots are completely normal elements and recall that we already have conditions to help us determine when $D_n(x,a) - b$ is irreducible over F_p, see [11]. Thus we're in business to construct some completely normal bases.

We also point out that when the polynomial $D_n(x,a) - b$ is irreducible over F_p, if α is a root of this polynomial, then we obtain a basis of F_{p^n} over F_p of the form $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, called a *polynomial basis.* This terminology arises from the fact that the elements of the extension field F_{p^n} may be viewed as polynomials in α of degree $< n$ with coefficients in F_p.

8 Combinatorics

For those readers with a combinatorial bent, we present two areas where Dickson polynomials play roles in combinatorics. If

$$(x)_n = x(x-1)(x-2)\cdots(x-n+1)$$

is the usual falling factorial, consider the expansion

$$x^n = \sum_{k=0}^{n} S(n,k)(x)_k, \qquad n = 0, 1, \ldots \tag{2}$$

where $S(n,k)$ denotes the Stirling number of the second kind. If $Z_n = \{1, 2, \ldots, n\}$ and $Z_m = \{1, 2, \ldots, m\}$, then as discovered by Stirling, with $x = m$ both sides of (2) count the number of functions from Z_n to Z_m. In [14] this was generalized to

$$D_n(x,a) - c_n = \sum_{k=0}^{n} S(n,k;a)(x|a)_k, \qquad n = 0, 1, \ldots$$

where

$$(x|a)_n = (x-a)(x-a-1)\cdots(x-a-n+1),$$

with $c_0 = 1$ and $c_k = 0$ for $k \geq 1$.

This provides a *Dickson-Stirling* number of the second kind. Moreover in [14] the following combinatorial refinement of Stirling's result above was obtained: Let $m \geq 1, n \geq 1$ and $0 \leq a < m$ be integers. Then $D_n(m,a) - D_n(a,a)$ counts the number of functions $f : Z_n \to Z_m$ that take at least one integer of the set $\{a+1, a+2, \ldots, m\}$, and such that no integer of Z_a occurs consecutively as an image in the cyclic sequence $f(1), f(2), \ldots, f(n), f(1)$.

Since for $a = 0$ there are no elements $\leq a$ in the range of any function f, we immediately obtain the case first discovered by Stirling. Other combinatorial results related to the Dickson-Stirling numbers are given in [14].

By a *latin square* of order n is meant an $n \times n$ array consisting of n distinct symbols with the property that each row and each column contains each of the n symbols exactly once. Two such squares are *orthogonal* if when superimposed, each of the n^2 possible ordered pairs occurs exactly once, and a set of squares is *orthogonal* if each pair of distinct squares is orthogonal.

Label the rows (and columns) of a $q \times q$ square with the elements of F_q, the field with q elements where $q = p^e$ with p prime and $e \geq 1$ an integer. For $b \in F_q^*$ and $(n, q^2-1) = 1$ (so that $D_n(x,b)$ permutes F_q), place the element

$$g_b(x,y) = bD_n(x,a) + D_n(y,a)$$

at the intersection of row x and column y of the b-th square. We leave it to the reader to check that this indeed gives a set of $q-1$ mutually orthogonal latin squares (MOLS) of order q. In fact it is not possible to construct more than $q-1$ MOLS of order q. Why is this? See Dénes and Keedwell [6] page 158. When $n = 1$ the above construction reduces to that of Bose [3] who also proved in the same paper that for a positive integer $m \geq 2$, there exist $m-1$ MOLS of order m if and only if there exists an affine plane $AG(2,m)$ of order m.

When q is a prime, a long standing conjecture postulates that any two affine planes of the same prime order are *desarguesian*, i.e. every set of $q-1$ MOLS of prime order q is equivalent to those constructed above. Here two sets of MOLS are *equivalent* if one set be obtained from the other by some fixed permutation of the rows, a (possibly different) permutation of the columns and a (possibly different) permutation of the symbols of the squares; see [6] pages 168 and 276.

9 Cryptographic applications

Ok, so you think all of these properties are rather theoretical in nature and of no practical significance at all. Wrong! We now briefly outline several practical applications of Dickson polynomials that involve various cryptographic systems for the secure transmission of information. We point out that cryptosystems are indeed widely used in today's information hungry society.

We first recall the very important RSA public key cryptosystem which is based upon the Dickson polynomial $D_n(x, 0) = x^n$. We choose two large primes p and q which are kept secret but their product $n = pq$ is made public. Assuming that Alice wants to send her friend Bob an important message m, Alice looks up in a public directory Bob's enciphering key e_B which is an integer with $(e_B, \phi(n)) = 1$, where $\phi(n)$ denotes Euler's function which counts the number of integers $< n$ which are relatively prime to n. Alice then enciphers her message m as $c \equiv m^{e_B} \pmod{n}$.

Since Bob knows the two primes p and q, he is able to solve the congruence $e_B d_B \equiv 1 \pmod{\phi(n)}$ for his private deciphering key d_B. Try finding $\phi(n)$ without knowledge of the two primes p and q whose product is n! Upon receiving c, in order to obtain the original message m Bob simply deciphers by calculating $c^{d_B} \equiv (m^{e_B})^{d_B} \equiv m \pmod{n}$.

We note that Alice can verify (*authenticate* is the fancy word) that the message came from her and not from one of Bob's many other girlfriends, i.e. Alice can *sign* her message. She simply calculates $m^{d_A} \equiv s \pmod{n}$. Bob knows that only Alice is able to obtain d_A (which she calculates analogously to the way Bob calculated d_B). Hence when Bob receives s he verifies that the message m came from Alice by calculating $s^{e_A} \equiv (m^{d_A})^{e_A} \equiv m \pmod{n}$.

As we by now expect, the general Dickson polynomial $D_n(x, a)$ with $a \neq 0$ can also be used in an analogous way to build a public key cryptographic system; see [16] section 7.1. We must however restrict our attention to the case where $a = 1$ in order that the Dickson polynomials are closed under composition. As in the earlier case we assume that Alice and Bob each have public enciphering keys e_A and e_B. Alice now enciphers her message m as $D_{e_B}(m, a) \equiv c \pmod{n}$, where $(e_B, (p^2 - 1)(q^2 - 1)) = 1$.

Bob calculates his deciphering key d_B from the congruence $e_B d_B \equiv 1 \pmod{(p^2 - 1)(q^2 - 1)}$ and then deciphers to obtain the original message m by calculating $D_{d_B}(c, a) \equiv m \pmod{n}$. In this setting Alice is able to also sign her messages; she simply begins the process by calculating $D_{d_A}(m, a) \equiv s \pmod{n}$, and Bob then calculates $D_{e_A}(s, a) \equiv D_{e_A}(D_{d_A}(m, a), a) \equiv m \pmod{n}$. See [16] section 7.1 for details.

How do Alice and Bob exchange a common key without the use of a courier? One method is to use the Diffie-Hellman key exchange system which works as follows, and which once again uses properties of Dickson polynomials. Choose a primitive element g in the field F_p. Alice has a secret integer a and so she sends to Bob the field element g^a who in turn with his secret integer b then calculates $(g^a)^b = g^{ab}$. Similarly Bob calculates g^b which is sent to Alice who calculates $(g^b)^a = g^{ba}$ and their common key is the field element $g^{ab} = g^{ba}$. This process is viewed as being quite safe since the *discrete logarithm problem* is generally believed to be difficult to solve. This problem asks for the value of t, given that you see the field element δ which we know to be written in the form $\delta = g^t$ where $0 \leq t < p-1$, and g is a primitive element in the field F_p.

You can devise an analogous Dickson key exchange system by taking $a = 1$. Why? We must however be a little more careful in choosing g which we take as in [16] to be $g = \gamma^{p-1} + \gamma^{-(p-1)}$, where γ is a primitive element in the field F_{p^2}. Alice calculates $D_a(D_b(g,1),1) = D_{ab}(g,1)$ and Bob calculates $D_b(D_a(g,1),1) = D_{ba}(g,1)$ and thus the common key is $D_{ab}(g,1) = D_{ba}(g,1)$. We refer to ([16], page 159) for details.

10 Conclusion

Hopefully by now you've come to the conclusion that the Dickson polynomials $\{D_n(x,a)\}$ are pretty interesting creatures. These are often called *Dickson polynomials of the first kind.* Are there other fascinating properties yet to be discovered? Most likely! For a survey of some algebraic and number theoretic properties as well as applications of Dickson polynomials, we refer to [16].

There is a closely related class of polynomials $E_n(x,a)$ called *Dickson polynomials of the second kind,* see [16]. They satisfy the same recurrence except that one changes the constant polynomial from $D_0(x,a) = 2$ to $E_0(x,a) = 1$. One might think that such a trivial change will not make life too difficult if one wants to develop properties of the Dickson polynomials $E_n(x,a)$ of the second kind. We leave it to you to see what analogous results you can obtain for these polynomials.

Acknowledgement. The second author would like to thank I. Shparlinski of Macquarie University for his hospitality during a visit when most of this paper was written.

References

[1] T.M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York-Heidelberg-Berlin, 1976.

[2] D. Blessenohl and K. Johnsen, *Eine Verschärfung des Satzes von der Normalbasis*, J. Algebra 103(1986), 141-159.

[3] R.C. Bose, *On the application of the properties of Galois fields to the construction of hyper-Graeco-Latin squares*, Sankhya 3(1938), 323-338.

[4] W.-S. Chou, J. Gomez-Calderon, and G.L. Mullen, *Value sets of Dickson polynomials over finite fields*, J. Number Thy. 30(1988), 334-344.

[5] S.D. Cohen, *Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials*, Canad. Math. Bull. 33(1990), 230-234.

[6] J. Dénes and A.D. Keedwell, Latin Squares and Their Applications, Academic Press, New York, 1974.

[7] L.E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. of Math. 11(1897). 65-120, 161-183.

[8] W. Diffie and M.E. Hellman, *New directions in cryptography*, IEEE Trans. Infor. Theory 22(1976), 644-654.

[9] G. Eisenstein, *Lehrsätze*, J. reine angew. Math. 39(1850), 180-182; Math. Werke, Chelsa, New York, Vol. 2, 1975, 620-622.

[10] M. Fried, *On a conjecture of Schur*, Michigan Math. J. 17(1970), 41-55.

[11] S. Gao and G.L. Mullen, *Dickson polynomials and irreducible polynomials over finite fields*, J. Number Thy. 49(1994), 118-132.

[12] J. Gomez-Calderon and D.J. Madden, *Polynomials with small value sets over finite fields*, J. Number Theory 28(1988), 167-188.

[13] K. Hensel, *Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor*, J. reine angew. Math. 103(1888), 230-237.

[14] L.C. Hsu, G.L. Mullen, and P.J.-S. Shiue, *Dickson-Stirling numbers*, Proc. Edinburgh Math. Soc. 40(1997), 409-423.

[15] H.W. Lenstra, Jr. and R.J. Schoof, *Primitive normal bases for finite fields*, Math. Comp. 48(1987), 217-224.

[16] R. Lidl, G.L. Mullen and G. Turnwald, Dickson Polynomials, Pitman Monographs and Surveys in Pure and Appl. Math., Vol. 65, Longman Scientific and Technical, Essex, England, 1993.

[17] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia Math. & Appl., Vol. 20, Cambridge Univ. Press, 1997.

[18] W.H. Mills, *Polynomials with minimal value sets*, Pacific J. Math. 14(1964), 225-241.

[19] G.L. Mullen, *Permutation polynomials: A matrix analogue of Schur's conjecture and a survey of recent results*, Finite Fields Appl. 1(1995), 242-258.

[20] K.V.H. Parshall, *A study in group theory: Leonard Eugene Dickson's Linear Groups*, The Math. Intelligencer 13, No. 1, (1991), 7-11.

[21] R.L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM 21(1978), 120-126.

[22] A. Scheerhorn, *Dickson polynomials and completely normal elements over finite fields*, In: Applications of Finite Fields, (D. Gollmann, Ed.), IMA Conf. Proc. Series, Oxford Univ. Press, Oxford, 1996, 47-55.

[23] I. Schur, *Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen*, Sitzungsber. Preuss. Akad. Wiss. Berlin, 1923, 123-134.

[24] G. Turnwald, *On Schur's conjecture*, J. Austral. Math. Soc., Ser. A 58(1995), 312-357.

[25] K.S. Williams, *A generalization of Cardan's solution of the cubic*, Math. Gaz. 46(1962), 221-223.

University of Tasmania, P.O. Box 1214, Launceston, Tasmania 7250, Australia, Email: rudi.lidl@utas.edu.au.

Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, U.S.A., Email: mullen@math.psu.edu.