$x^n + x + a$

V. Kumar Murty and Shuyang Shen
University of Toronto

Talk at Mathfest 2019

August 1, 2019
We are going to study properties of the family of polynomials $x^n + x + a$

for different $n$ and $a$.

- This started a few years ago as an undergraduate summer project but has grown beyond that.
- A lot of interesting mathematics can be introduced through a study of these polynomials.
How is this connected to cryptography?

- A large part of what has been discussed so far takes place in the context of finite fields.
- Implementation requires an explicit representation of the elements of a finite field.
- Given a prime \( p \), a finite field \( \mathbb{F}_p \) of \( p \) elements and an irreducible polynomial \( f(x) \in \mathbb{F}_p[x] \) of degree \( n \), the quotient
  \[
  \mathbb{F}_p[x]/(f(x))
  \]
  is a finite field of \( p^n \) elements.
- Its elements can be represented by polynomials
  \[
  a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}
  \]
  where \( a_0, \cdots, a_{n-1} \in \mathbb{F}_p \).
Addition and multiplication of these elements is done modulo $f(x)$.

If $f(x)$ is *lacunary*, the arithmetic is more efficient.
If $x^n + x + a$ is irreducible modulo $p$, then we can use it to generate a finite field in which arithmetic is very efficient.

For such a polynomial to be irreducible modulo $p$, it must first be irreducible over the rationals $\mathbb{Q}$.

And this is the launching point for a lot of interesting (and difficult and unsolved) problems.

For which values of $n$ and $a$ is $x^n + x + a$ irreducible over $\mathbb{Q}$?

Solved for $a = 1$.

For other values, we have only statistical results.
The case $x^n + x + 1$

Theorem (Selmer, 1956)

The polynomial $x^n + x + 1$ is irreducible if $n \not\equiv 2 \pmod{3}$. Moreover, if $n \equiv 2 \pmod{3}$, it is divisible by $x^2 + x + 1$ and the quotient is irreducible.

Outline of Selmer’s argument

- For any polynomial $f$ with integer coefficients and having only non-zero roots, we introduce the invariant
  \[ S(f) = \sum_{i=1}^{n} \left( \rho_i - \frac{1}{\rho_i} \right) \]
  where $\rho_1, \cdots, \rho_n$ are the roots of $f(x)$.
- It is easy to see that $S(f)$ is a rational number by comparing with the coefficients.
- If the leading and constant coefficients of $f$ are $\pm 1$, then it is in fact an integer.
If $f = gh$ is a factorization, then

$$S(f) = S(g) + S(h).$$

If the constant term of $f$ is $\pm 1$, then in any factorization $f = gh$, the constant term of the factors is still $\pm 1$ and so $S(g)$ and $S(h)$ are integers.

For $f(x) = x^n + x + 1$, we have $S = S(f) = 1$.

Hence, if $f = gh$, then $S(g)$ and $S(h)$ are integers satisfying $S(g) + S(h) = 1$. 
On the other hand, writing each root as $\rho_i = r_i e^{i\phi_i}$, and grouping together complex conjugate roots, we have

$$S = \sum_{0<\phi_i<\pi} * \frac{2r_i^2 - 1}{r_i} \cos \phi_i$$

where the asterisk on the sum means that the factor 2 is suppressed for real roots (for which $\cos \phi = \pm 1$).
Outline of Selmer’s argument

- If $z = re^{i\phi}$ is a root of $x^n + x + 1$, separating real and imaginary parts gives

  $$r^n \cos n\phi = -(r \cos \phi + 1) \quad \text{and} \quad r^n \sin n\phi = -r \sin \phi.$$ 

- From this we deduce that

  $$\cos \phi = \frac{r^{2n} - r^2 - 1}{2r}.$$
Outline of Selmer’s argument

- Using this formula

\[ 2 \frac{r_i^2 - 1}{r_i} \cos \phi_i = 2 \left( \frac{r_i^2 - 1}{r_i} \right) \left( \frac{r_i^{2^n} - r_i^2 - 1}{2r_i} \right) \]
\[ = \frac{1}{r_i^2} - r_i^2 + r_i^{2n-2}(r_i^2 - 1) \]
\[ \geq \frac{1}{r_i^2} - 1 \]  

(1)\\

(2)

since

\[ r_i^{2n-2}(r_i^2 - 1) \geq r_i^2 - 1 \]

with equality if and only if \( r_i = 1 \).
Hence, we have

\[ S \geq \frac{1}{2} \sum \left( \frac{1}{r_i^2} - 1 \right) \]

where now the sum is over all roots (real and complex).

On the other hand, the product of the modulus of the roots is equal to 1.

Now use the arithmetic mean - geometric mean inequality

\[ \frac{1}{n} \sum_i \frac{1}{r_i^2} \geq \left( \prod_i \frac{1}{r_i^2} \right)^{1/n} = 1 \]

to deduce

\[ S \geq 0. \]
Equality holds in the above if and only if all $r_i$ are equal, and hence equal to 1.

If all $r_i = 1$, then $\cos \phi_i = -\frac{1}{2}$ so $\phi_i = \frac{2\pi}{3}$ for all $i$.

This means that

$$\rho_i = e^{\frac{2\pi i}{3}}.$$

Since $\rho_i^2 + \rho_i + 1 = 0$ and $\rho_i^n + \rho_i + 1 = 0$, it follows that $n \equiv 2 \pmod{3}$.
Theorem

The polynomial \( f(x) = x^n + x + p \) is irreducible for any prime \( p \geq 3 \).

Proof.

Suppose it has factors \( g(x)h(x) \), then one of them has constant term 1. Hence, at least one complex root has norm \( \leq 1 \). If \( z \) is such a root, then

\[
|z^n + z| \leq |z|^n + |z| \leq 2 < p
\]

which is a contradiction.
Motivated by the case of $n = 2, 3$, we might expect the following to be true.

**Conjecture**

\[
\#\{a: 0 < a \leq T, \ x^n + x + a \text{ is irreducible}\} = T + O(T^{1/n}).
\]

The result of the last slide shows that the left hand side is $\gg T/\log T$.

Effective Hilbert Irreducibility gives the asymptotic formula with an error of $O(T^{1/2})$. 
The Galois group

Theorem (Nart-Vila (1979), Osada (1987))

If

\[ f(x) = x^n + x + a \]

is irreducible and \((n - 1, a) = 1\), then its Galois group is \(S_n\).

E. Nart and N. Vila, Equations of the type \(X^n + aX + b\) with absolute Galois group \(S_n\), Rev. Univ. Santander, 11(1979), 821-825.

If $x^n + x + a$ has Galois group $S_n$, we can use Chebotarev to deduce that there are lots of primes for which it stays irreducible modulo $p$.

Assuming the Riemann Hypothesis, there is such a prime $\ll (\log D(n, a))^2$ where $D(n, a)$ is the discriminant of the polynomial.

We have

$$D(n, a) = (-1)^{n(n-1)/2} (n^n a^{n-1} + (1 - n)^{n-1}).$$

Thus,

$$\left(\log D(n, a)\right)^2 \ll (n \log an)^2.$$
Arithmetic properties of $D(n, a)$

- The numbers $D(n, a)$ seem to have interesting properties.
- Not only do they grow very fast, but their largest prime factor also seems to grow fast.
## Factorization of $D(n, 1)$ for $n < 20$

| $n$ | $|D(n, 1)|$ | $n$ | $|D(n, 1)|$ |
|-----|------------|-----|------------|
| 2   | 3          | 11  | $3(37^2)(8017)(8969)$ |
| 3   | 31         | 12  | $(5)(89)(19395030961)$ |
| 4   | 229        | 13  | $(7)(17)(47)(277)(1723)(116803)$ |
| 5   | $3(7^2)(23)$ | 14  | $(3)(61^2)(968299894201)$ |
| 6   | $(101)(431)$ | 15  | $(7334881)(61215157711)$ |
| 7   | $(11)(239)(331)$ | 16  | $(109)(165218809021364149)$ |
| 8   | $3(19^2)(14731)$ | 17  | $(3)(7^2)(13^2)(34041259347101651)$ |
| 9   | $(5)(197)(410353)$ | 18  | $(9680119)(3979203955386313)$ |
| 10  | $(29)(4127)(80317)$ | 19  | $(149)(2063)(6564253087266573169)$ |
Factorization of $D(n, 2)$ for $n < 20$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$D(n, 2)$</th>
<th>$n$</th>
<th>$D(n, 2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>7</td>
<td>11</td>
<td>$(2^{12})(3^2)(757)(10469743)$</td>
</tr>
<tr>
<td>3</td>
<td>$(2^4)(7)$</td>
<td>12</td>
<td>$(89)(1429)(17509)(8200013)$</td>
</tr>
<tr>
<td>4</td>
<td>$(43)(47)$</td>
<td>13</td>
<td>$(2^{12})(7^2)(11)(561924458951)$</td>
</tr>
<tr>
<td>5</td>
<td>$(2^4)(3^2)(349)$</td>
<td>14</td>
<td>$(17)(18223)(1303411)(225439919)$</td>
</tr>
<tr>
<td>6</td>
<td>$1489867$</td>
<td>15</td>
<td>$(2^{20})(19)(23)(181)(86502681953)$</td>
</tr>
<tr>
<td>7</td>
<td>$(2^{10})(51517)$</td>
<td>16</td>
<td>$604462471913424206493713$</td>
</tr>
<tr>
<td>8</td>
<td>$(5)(271)(293)(5407)$</td>
<td>17</td>
<td>$(2^{16})(3^4)(11)(928440564939745763)$</td>
</tr>
<tr>
<td>9</td>
<td>$(2^8)(5^2)(15499441)$</td>
<td>18</td>
<td>$(11)(16535393879261)(28353568052881)$</td>
</tr>
<tr>
<td>10</td>
<td>$(1249)(4098969239)$</td>
<td>19</td>
<td>$(2^{20})(5^2)(4561)(4337688677384233471)$</td>
</tr>
</tbody>
</table>
Distribution of largest prime factors of $D(n, 1)$

Figure: $(n, \log P(D(n, 1)))$
A conditional lower bound

Theorem (M+Shen)

Assume the ABC conjecture. Then

\[ P(D(n, a)) \gg n \log na. \]
The ABC conjecture

Conjecture

(Masser-Oesterle) If \( a + b + c = 0 \), and \( a, b, c \) are pairwise coprime, then for any \( \epsilon > 0 \),

\[
\max\{|a|, |b|, |c|\} \ll \epsilon \left( \prod_{p | abc} p \right)^{1+\epsilon}
\]

It has amazing consequences.
We started from a cryptographically inspired problem.
It quickly led to other problems which are not directly connected to cryptography, but which are mathematically interesting and difficult.
The lesson is that the pure and applied aspects of mathematics are mutually stimulating.