Cryptography and Schur's Conjecture

UM Bozeman, November 19, 2004

Advertisement for our seminar at MSU-Billings.

"WHAT-DO-YOU-KNOW? MATHEMATICS COLLOQUIUM:"

We plan talks this year on historical topics with serious mathematical use today. The language and tradition of Mathematics thrives on problems that excite researchers even though they remain unsolved for half a century or longer. While unsolved, such problems can be a bottleneck to progress because mathematics deals with that for which we have no senses: What we consider abstract. These talks will present tools that can remove the abstractness that halts progress.

Abstract: Galois, finite fields and nonabelian Galois Theory

I will define capitalized words during the talk:

In 1831, 19 year old Everiste Galois introduced **FINITE FIELDS**. The easiest are PRIME finite fields: Integers modulo a prime. You may know bankers who never heard of Galois, yet they know of cryptography and finite fields. Addition and multiplication on these keep financial data secure.

Numbers in a finite field form an **ABELIAN group**. The nonzero numbers form a **CYCLIC** group. This allows encoding data using special polynomials: the easiest being odd degree **CYCLIC POLYNOMIALS** x^3, x^5, ... In 1919 (1923), Group theorist Isaiah Schur guessed at a complete list of polynomials that could encode data in large prime finite fields. We explain why Schur's guess (solved in 1969, after hundreds of partial results) was correct. Main tools are **NONABELIAN GALOIS THEORY**, also introduced by Galois, and complex variables. Recent large manuscripts start from this. We conclude with why it is timely to revisit this.

1. Cyclic polynomials used in Cryptography:

Cyclic polynomials have the form $x \longrightarrow x^n$.

The famous R(ivest)S(hamir)A(dleman) code scheme uses these. Fewer people know about Chebychev polynomials. Yet, these also have their cryptography use. Often we can use compositions of these two types.

Proposition 1. *If* $(n, p-1) = 1$, *then we can use* x^n *to scramble data into* $\mathbb{Z}/p$. *If* n *is odd, there are infinitely many such primes* p.

Proof. Euler's Theorem: Powers of a single integer α fill out $\mathbb{Z}/p \setminus \{0\} \stackrel{\text{def}}{=} \mathbb{Z}/p^*$.

Example: $2, 2^2 = 4, 2^3 \equiv 3, 2^4 \equiv 1 \mod 5$. Subexample of $(n, 4) = 1$: $n = 1 + s \cdot 4$. Then $2^{u \cdot n} = (2 \cdot (2^4)^s)^u \equiv 2^u \mod 5$. □

Primes that work and Chebychev polynomials

Take $p \in \{k + m \cdot n | m \in \mathbb{Z}\}$ where k satisfies:

- $(k, n) = 1$ (apply Dirichlet's Theorem); and

- $(k-1, n)$ (so $(p-1 = k-1+m \cdot n, n) = 1$).

Example: $k = 2$ works; other integers may too.

Tchebychev polynomials:

$$T_n(x + 1/x) = x^n + 1/x^n.$$

Proposition 2. *If* $(n, 6) = 1$, *then* T_n *maps* $\mathbb{Z}/p \to \mathbb{Z}/p$ *for infinitely many* p. *Exactly those primes* p *with* $(p^2 - 1, n) = 1$.

Proof: Use finite fields $\mathbb{F}_{p^2} \supset \mathbb{Z}/p$: $\mathbb{F}^*_{p^2}$ cyclic.

2. Schur's Conjecture:

Cryptography we recognize in modern algebra goes back to the middle of the 1800s. They used finite fields as the place to encode a message. Schur 1919: Famous conjecture about polynomials $f(x)$ that could embed arbitrary data in infinitely many residue fields ($\mathbb{Z}/p$s).

Conjecture 3. Only compositions of cyclic, Tchebychev and degree 1 ($x \mapsto ax + b$) give polynomials mapping 1-1 on $\mathbb{Z}/p$ for ∞ of p.

Problem 4. How to check if an $f(x)$ is a composition of the correct polynomials? If so, how to check it is 1-1 for ∞ of p (notation: 1–1_∞)?

3. Points toward proving Schur's conjecture:

Step 1: If $f = f_1 \circ f_2$, then f is 1–1$_\infty$ if and only f_1 *and* f_2 are 1–1$_\infty$. Subtle reduction: If f decomposes over the complex numbers then it decomposes over $\mathbb{Q}$. So, to prove Schur's conjecture we consider f *indecomposable*.

Step 2: Consider 1–1$_\infty f$: p with $f : \mathbb{Z}/p \to \mathbb{Z}/p$ 1-1. Then, the polynomial expression

$$\phi(x, y) = \frac{f(x) - f(y)}{x - y} = 0$$

has no solutions $(x_0, y_0) \in \mathbb{Z}/p \times \mathbb{Z}/p$, $x_0 \neq y_0$.

Proposition 5 (Weil). *If $\phi(x, y)$ has u absolutely irreducible factors, then it has $u \cdot p + A\sqrt{p}$ solutions (A constant in p).*

Corollary 6. *If f is 1–1$_\infty$, then $\phi(x, y)$ has no absolutely irreducible factors.*

MONODROMY GROUP of f that is 1–1$_\infty$.

Consider $f(x) - z = 0$ with z a variable. Solve this in some algebraic closure F of $\mathbb{Q}(z)$: There are n solutions $x_1, \ldots, x_n$: $f(x_i) = z$; they generate a field $\mathbb{Q}(x_1, \ldots, x_n, z) \stackrel{\text{def}}{=} L_f$.

Definition 7. Among permutations of $x_1, \ldots, x_n$ (elements in S_n), a subset called G_f, gives field automorphisms of L_f: It is closed under composition, and forms a group.

Proposition 8. *Then, $G_f \leq S_n$ is primitive, not doubly transitive, and contains an n-cycle.*

Example 9. Assume $n > 2$ is prime. The group D_n (Dihedral of degree n) with generators

$$\begin{aligned} g_1 &= (1\,n)(2\,n{-}1)\cdots(\tfrac{n-1}{2}\,\tfrac{n+3}{2}) \\ g_2 &= (2\,n)(3\,n{-}1)\cdots(\tfrac{n+1}{2}\,\tfrac{n+3}{2}) \end{aligned}$$

is primitive, not double transitive, has an n-cycle.

Reasons for primitive, n-cycle, and not doubly transitive.

Why an n-cycle?: Write

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n.$$

Solve for x from $f(x) = z$. One solution:

$$x_1 = z^{1/n} + b_0 + b_1 z^{-1/n} + b_2 z^{-2/n} + \cdots .$$

Others by substituting $e^{\frac{2\pi i \cdot k}{n}} z^{\frac{1}{n}} \mapsto z^{1/n}$.
Gives an n-cycle automorphism of L_f.

Why primitive?: Let $G_f(x_1)$ be the subgroup of G_f fixing x_1. Primitive means no groups H with $G_f(x_1) < H < G_f$. Galois correspondence: Such an H would mean a field $L = \mathbb{Q}(w)$ with $\mathbb{Q}(z) < L < \mathbb{Q}(x_1)$. So, $w = f_2(x_1)$, and $z = f_1(w)$. Contrary to indecomposable f:

$$f_1(f_2(x_1)) = z.$$

Why G_f is not doubly transitive: Equivalent to $\phi(x, y)$ factors over $\bar{\mathbb{Q}}$.

4. Combine Groups – Complex Variables:

Schur's conjecture follows if 1–1_∞ indecomposable polynomial f is cyclic or Chebychev.

Step 1: Show G_f is a cyclic or dihedral group.
Proposition 10 (Famous Group Results). *If n is a prime, then (Burnside):*

$$G_f \leq \left\{ \begin{pmatrix} u & v \\ 0 & 1 \end{pmatrix} \mid u \in \mathbb{Z}/n^*, v \in \mathbb{Z}/n \right\} \stackrel{\text{def}}{=} \mathbb{Z}/n \times^s \mathbb{Z}/n^*.$$

For n not prime there is no such G_f: Schur.

Step 2: Show G_f dihedral (resp. cyclic) $\Longleftrightarrow$ f is Chebychev (resp. cyclic) after changing variables. Niftiest part: Allows solving many other problems (Schur's conjecture the easiest).

For $g \in S_n$, $\text{ind}(g) = n - t$ with t the number of disjoint cycles.

Step 2 cont: Apply Riemann's Existence Theorem.

If $f : \mathbb{C}_x \to \mathbb{C}_z$, with branch points $z_1, \ldots, z_r$, then there are r elements $g_1, \ldots, g_{r-1}, g_\infty \in S_n$ (*branch cycles*) with these properties:

- g_∞ an n-cycle;
- $G_f = \langle g_1, \ldots, g_{r-1} \rangle$ (generation);
- $(\prod_{I=1}^{r-1} g_i) g_\infty = 1$ (product-one); and
- $n - 1 = \sum_{i=1}^{r-1} \mathrm{ind}(g_i)$ (genus 0).

Proposition 11. *Combine with*

$$g_1, \ldots, g_{r-1}, g_\infty \in \mathbb{Z}/n \times^s \mathbb{Z}/n^*.$$

Result:

- $g_1, \ldots, g_{r-1} = g_1, g_2$ *(Ex. 9),* $g_\infty = (1\,2\,\ldots\,n)^{-1}$*; or*
- $r = 2$ *and* $g_1 = (1\,2\,\ldots\,n)$.

Tchebychev/cyclic polynomial branch cycles.

5. What happened with the bottleneck of Schur's conjecture proved?:

Once people knew what polynomials would enable cryptography, they asked what rational functions would. Most new functions from Weierstrass $\wp$-functions through this diagram:

$$\begin{array}{ccc} \mathbb{C}_{\{\pm w\}} \cup \{\infty\} & \xrightarrow{f} & \mathbb{C}_{\{\pm z\}} \cup \{\infty\} \\ \text{mod } \{\pm 1\} \uparrow & & \uparrow \text{ mod } \{\pm 1\} \\ \mathbb{C}_w/L_w & \xrightarrow{\text{mod } L_z/L_w} & \mathbb{C}_z/L_z. \end{array}$$

Here $L_w \leq L_z$ are both generated by two linearly independent complex numbers.

Problem 12. Which fs useful to cryptography? Full answer generalizes famous theorem of Serre on modular curves. Given f, finding embedding primes p has unsolved aspects.

Bibliography:

- [Fr70] M.D. Fried, *On a conjecture of Schur*, Mich. Math. J. **17** (1970), 41–45.
- [Fr78] M. Fried, *Galois groups and Complex Multiplication*, T.A.M.S. **235** (1978) 141–162.
- [GMS03] R. Guralnick, P. Müller and J. Saxl, *The rational function analoque of a question of Schur and exceptionality of permutations representations*, Memoirs of AMS **162** 773 (2003),ISBN 0065-9266.
- [LMT93]R. Lidl, G.L. Mullen and G. Turnwald, *Dickson Polynomials*, Pitman monographs, Surveys in pure and applied math,**65**, Longman Scientific, 1993.
- [Sch23] I. Schur, Über den Zusammenhang zwischen einem Problem der Zahlentheorie and einem Satz über algebraische Functionen, S.-B. Preuss. Akad. Wiss., Phys.-Math. Klasse (1923), 123–134.
- [Se68] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, 1st ed., McGill University Lecture Notes, Benjamin, New York • Amsterdam, 1968, in collaboration with Willem Kuyk and John Labute.
- [Se81] J.-P. Serre, *Quelques Applications du Théorème de Densité de Chebotarev*, Publ. Math. IHES **54** (1981), 323–401.