Introduction to Number Fields

David P. Roberts
University of Minnesota, Morris

1. The factpat problem
2. Polynomial discriminants
3. Global factorizations
4. Generic factorization statistics
5. Resolvents revealing non-genericity
6. Galois groups
7. Number fields
8. Field discriminants
9. Local invariants
10. The factpat problem revisited

1. The factpat problem. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial. For every prime p, one can reduce it to $f_p(x) \in \mathbb{F}_p[x]$ and factor it into irreducibles. Let λ_p be the object capturing degrees and multiplicities as in the example of $f(x) = x^7 - 7x - 3$:

p	$f_p(x)$	λ_p
2	$x^7 + x + 1$	7
3	$(x+1)^3(x+2)^3x$	$\boxed{1^3\,1^3\,1}$
5	$x^7 + 3x + 2$	7
7	$(x+4)^7$	$\boxed{1^7}$
11	$x^7 + 4x + 8$	7
13	(quart) $\left(x^2 + 12x + 2\right)(x+2)$	4 2 1
17		3 3 1
19		3 3 1
23		3 3 1
29		7

A natural and very large question is the "factpat" problem: *what can be said about the sequence* $\lambda_2, \lambda_3, \lambda_5$ *... in general?* The central role in the ongoing effort to respond to this question is played by *number fields*.

2. Polynomial Discriminants. We say that a factor is *bad* if the multiplicities are greater than 1, as in $1^3\,1^3\,1$ or 1^7. We say it is *good* otherwise, in which case the symbol λ_p is just a partition of the degree n.

The distinction bad vs. good can easily understood via the *polynomial discriminant* of $f(x)$ defined via its complex roots α_i as

$$D_f = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in \mathbb{Z}.$$

As an example, $D_{x^7-7x-3} = 3^8 7^8$.

In general,

$$p \text{ is bad} \iff p \mid D_f.$$

Henceforth we restrict attention to *separable* f, meaning f with distinct roots, or equivalently f with $D_f \neq 0$. Then there are only finitely many bad primes.

3. Global factorizations. Suppose $f(x) \in \mathbb{Z}[x]$ factors into irreducibles as $\prod f_i(x)$. Then for all primes there are induced factorizations $f(x) = \prod_i f_{i,p}(x)$. At a good prime p there is a corresponding factorization $\lambda_p = \prod \lambda_{i,p}$. For example, the bad primes for

$$f(x) = x^5 + 3x^3 + 2x^2 + 6$$

are 2, 3, and 31. The factor partitions for the first 100 good primes have the following statistics

λ	#	λ_1	λ_2
2 2 1	51	2 1	2
3 1 1	32	3	1 1
1 1 1 1 1	14	1 1 1	1 1

Only three of the seven partitions of five have arisen in the λ column. This behavior is in part trivially explained by the factorization

$$f(x) = (x^3 + 2)(x^2 + 3).$$

Because of this simple phenomenon, one focuses mainly on irreducible f.

4. Generic factorization statistics. A key insight into the factpat problem concerns generic degree n polynomials $f(x)$. Here the frequency that a partition λ arises as λ_p is asymptotically the same as the frequency it arises as the cycle structure λ_g of $g \in S_n$. Examples with $n = 7$ and the first $7! = 5040$ primes:

λ	# of g in S_7	# of p for $x^7 - 7x - 4$	# of p for $x^7 - 7x - 3$
7	720	749	1448
43	420	423	
52	504	499	
61	840	865	
322	210	174	
331	280	261	1687
421	630	659	1271
511	504	501	
2221	105	104	
3211	420	389	
4111	210	214	
22111	105	116	604
31111	70	67	
211111	21	14	
1111111	1	1	28

5. Resolvents confirming non-genericity. The non-generic behavior of $x^7 - 7x - 3$ is explained by the factorization of a resolvent built from its roots:

$$\begin{aligned} g(x) &= \prod_{i<j<k} (x - (\alpha_i + \alpha_j + \alpha_k)) \\ &= (x^7 - 14x^4 + 42x^2 - 21x - 9) f_{28}(x) \end{aligned}$$

In general, any deviation of a degree n polynomial from S_n statistics is caused by the non-generic factorization of some resolvent.

The statistics governing factpats for $x^7 - 7x - 3$ are those coming from the transitive permutation group $GL_3(\mathbb{F}_2) \subset S_7$ of order 168. Computing with 168, 1680, 16800, and 168000 primes gives the following data:

λ	168	1680	16800	168000
7	40	47.6	48.16	48.085
331	58	56.3	56.14	55.956
421	46	43.6	41.97	41.909
22111	22	19.4	20.78	21.085
1111111	0	0.9	0.93	0.963

6. Galois groups. The groups S_7 and $GL_3(\mathbb{F}_2)$ appearing on the last two slides are examples of Galois groups. In general, let $f(x) \in \mathbb{Q}[x]$ be a separable polynomial with complex roots α_1, . . . , α_n. Let

$$F_f^{\mathrm{gal}} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subset \mathbb{C}$$

be its splitting field. Let Gal$(F_f^{\mathrm{gal}}/\mathbb{Q})$ be its group of automorphisms. One can think of Gal$(F_f^{\mathrm{gal}}/\mathbb{Q})$ as the group of permutations of the roots which preserve all algebraic relations.

The Chebotarev density theorem says that good factorization patterns are asymptotically distributed according to the cycle types of elements in Gal$(F_f^{\mathrm{gal}}/\mathbb{Q})$. This works for reducible polynomials as well. For example, the statistics of the factorization of $(x^3 + 2)(x^2 + 3)$ are governed by its six-element Galois group $S_3 \times S_2 \cap A_5$.

7. Number fields. A fundamental phenomenon not discussed so far is that two different polynomials can have the same factorization patterns at their common good primes for completely trivial reasons.

To work more intrinsically, we focus not on the given separable polynomial $f(x)$, but rather on its associated *number algebra*

$$F = \mathbb{Q}[x]/f(x)$$

The good factorization patterns of $f(x)$ are invariants of F.

The factorization $f(x) = \prod f_i(x)$ into irreducibles induces a factorization $F = \prod F_i$ into *number fields*, where $F_i = \mathbb{Q}[x]/f_i(x)$.

The set of roots of $f(x)$ canonifies into the set $\mathrm{Hom}(F, \mathbb{C})$ of homomorphisms from F into $\mathbb{C}$. Thus F_f^{gal} depends only on F and and can be denoted F^{gal}. When F is a field, all the homomorphisms are embeddings. At the other extreme, for $F = \mathbb{Q}^n$, one has $F^{\mathrm{gal}} = \mathbb{Q}$.

8. Field discriminants In the shift of focus from polynomials f to algebras F, the polynomial discriminant D_f is lost. An ideal substitute is the field discriminant d_F as follows.

An element k in a number algebra F has a minimal polynomial $f_k(x) \in \mathbb{Q}[x]$, namely the unique monic polynomial of smallest degree with $f_k(k) = 0$. In fact, as k runs over generators of F, the minimal polynomials run over defining polynomials of F.

The element k in a number algebra F is called *integral* if its minimal polynomial $f_k(x)$ is in $\mathbb{Z}[x]$. The set of integral elements form a subring $\mathcal{O}$ of F. For any algebraic integer k generating F, the index $c_f = [\mathcal{O} : \mathbb{Z}[k]]$ is finite. The quantity

$$d_F = D_f/c_f^2$$

is independent of f and is the field discriminant of F. One source of its importance is $\mathcal{O}$ sits as a lattice inside $F_\infty = \mathbb{Q} \otimes \mathbb{R}$, and $\sqrt{|d_F|}$ is the volume of the quotient torus $F_\infty/\mathcal{O}$.

9. Local invariants. We can now be more sophisticated about the factpats λ_p. Let F be a number algebra, typically a number field in practice. Let $v \in \{\infty, 2, 3, 5, \ldots\}$ be a place of $\mathbb{Q}$. Let $F_v = F \otimes_{\mathbb{Q}} \mathbb{Q}_v$ be its v-adic completion.

For $v = \infty$, one necessarily has $F_v = \mathbb{R}^r \times \mathbb{C}^s$ with $r + 2s = n$. One can define $\lambda_\infty = 2 \ldots 2\, 1 \ldots 1$ in analogy with other λ_p.

For $p \nmid d$, the algebra F_p is unramified. If $\lambda_p = f_1 \cdots f_k$ then $F_p \cong \mathbb{Q}_{p^{f_1}} \times \cdots \times \mathbb{Q}_{p^{f_k}}$ with $\mathbb{Q}_{p^f}$ the unramified degree f extension of $\mathbb{Q}_p$.

For $p|D$, the situation is more complicated. But still F_p factors into fields and each field has a residual degree f, a ramification index e, and a local discriminant c. We use the f_c^e to *redefine* λ_p, so that for the Trinks field one now has $\lambda_3 = 1_3^3\, 1_3^3\, 1$ and $\lambda_7 = 1_8^7$.

10. The factpat problem revisited. With the slightly modified λ_v, the factpat problem now is now asking for a classification of number fields (up to arithmetic equivalence rather than isomorphism, with e.g. $\mathbb{Q}[x]/(x^7 - 7x - 3)$ and its dual $\mathbb{Q}[x]/(x^7 - 14x^4 + 42x^2 - 21x - 9)$ being non-isomorphic but having the same factpats).

Focusing on the main invariants d and G only, one can ask for the set $NF(d, G)$ of all number fields with discriminant d and Galois group $G \subseteq S_n$. **1)** These are finite sets. **2)** They can be effectively tabulated for n small via computer searches. **3)** They can be effectively tabulated for G solvable and of moderate size, via class field theory. **4)** They can be pursued for say $G \subseteq PGL_2(\mathbb{F}_{\ell^f})$ via automorphic forms. **5)** Their size for G fixed and $|d|$ increasing is expected to obey simple asymptotics, proved for some G. **6)** The symbols λ_v are naturally packaged into a zeta function $\zeta_F(s)$, and one expects that all λ_v can be determined analytically from a sufficiently large initial segment.