

Fermat vs Waring: An Introduction to Number Theory in Function Fields

Sachin Kumar

Univeristy of Waterloo, Faculty of Mathematics

Abstract

Let \mathbb{Z} be the ring of integers, and let $\mathbb{F}_p[t]$ be the ring of polynomials in one variable defined over the finite field \mathbb{F}_p of p elements. Since the characteristic of \mathbb{Z} is 0, while that of $\mathbb{F}_p[t]$ is the positive prime number p , it is a striking theme in arithmetic that these two rings faithfully resemble each other. The study of the similarity and difference between \mathbb{Z} and $\mathbb{F}_p[t]$ lies in the field that relates number fields to function fields. In this talk, we will investigate some Diophantine problems in the settings of \mathbb{Z} and $\mathbb{F}_p[t]$, including Fermat's last theorem and Waring's problem. This essay will be presented in five sections: Fermat's last theorem and Waring's problem in \mathbb{Z} ; An Analogies between \mathbb{Z} and $\mathbb{F}_p[t]$; Fermat's last theorem in $\mathbb{F}_p[t]$, Waring's problem in $\mathbb{F}_p[t]$ and Taylor Series in $\mathbb{F}_p[t]$.

1. Fermat's Last Theorem and Waring's problem in \mathbb{Z}

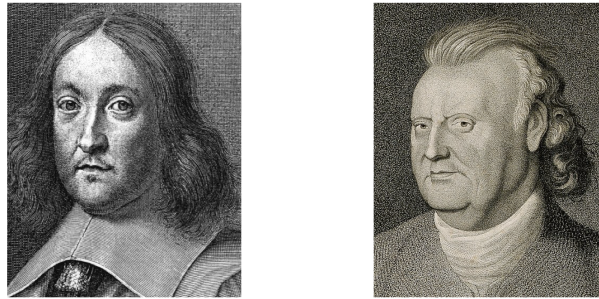


Figure 1: Pierre de Fermat and Edward Waring

From middle school, we have heard about the Pythagorean Theorem,

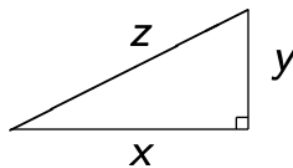


Figure 2: Pythagorean Triangle

We have

$$x^2 + y^2 = z^2$$

The triples $(x, y, z) = (3, 4, 5)$ and $(5, 12, 13)$ are primitive solutions.

Euclid's Formula. Let $\mathbb{N} = \{1, 2, \dots\}$. $\forall a, b \in \mathbb{N}$ with $a > b$, we can take

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2$$

Finding all right triangles with integer side-lengths is equivalent to solving the Diophantine equation $x^2 + y^2 = z^2$.


Question. How about $x^n + y^n = z^n$ with $n \in \mathbb{N}$ and $n \geq 3$?

Fermat's Last Theorem. For $n \in \mathbb{N}$ with $n \geq 3$, the equation $x^n + y^n = z^n$ has no solution with $x, y, z \in \mathbb{N}$.


The theorem was proved by Frey, Serre, Ribet, Taylor and Wiles in 1994. The proof involves the use of elliptic curves, modular forms and Galois representations.

In Euclid's formula, we set $z = a^2 + b^2$.

Question. Can we get all positive integers z in this way?

Solution. No, since $3 \neq a^2 + b^2$ with $a, b \in \mathbb{N}$. More generally, since $a^2 \equiv 0, 1 \pmod{4}$ and $b^2 \equiv 0, 1 \pmod{4}$, we can only get those $z \in \mathbb{N}$ with $z \equiv 0, 1, 2 \pmod{4}$. 

Question. Can we get all positive integers using more variables?

Idea. $1 = 1^2$, $2 = 1^2 + 1^2$, $3 = 1^2 + 1^2 + 1^2$, $4 = 2^2$, $5 = 2^2 + 1^2$, $6 = 2^2 + 1^2 + 1^2$, $7 = 2^2 + 1^2 + 1^2 + 1^2$, $8 = 2^2 + 2^2$, $9 = 3^2$, \dots , $2023 = 37^2 + 25^2 + 5^2 + 2^2$, \dots 

Question. Can we write all positive integers as a sum of at most four squares? More generally, for $k \in \mathbb{N}$ with $k \geq 2$, can we write all positive integers as a sum of a bounded number of k^{th} powers?

Waring's Problem. For $k \in \mathbb{N}$ with $k \geq 2$, can we find an integer $s = s(k)$ such that for all $n \in \mathbb{N}$, there exists $x_1, \dots, x_s \in \mathbb{N} \cup \{0\}$ with

$$n = x_1^k + x_2^k + \dots + x_s^k = \sum_{i=1}^s x_i^k$$

Let $g(k)$ denote the least integer $s = s(k)$ such that the above equation holds for all $n \in \mathbb{N}$. In 1770, Lagrange proved $g(2) = 4$. Before 1909, only known cases are $k = 2, 3, 4, 5, 6, 7, 8, 10$. In 1909, Hilbert proved that $g(k) < \infty$ for every $k \geq 2$.

Consider

$$n = 2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 < 3^k$$

For the most efficient way to represent n : Use $\left(\left\lfloor\left(\frac{3}{2}\right)^k\right\rfloor - 1\right)$ copies of 2^k and $(2^k + 1)$ copies of 1^k . Thus we obtain a result of Euler that

$$g(k) \geq 2^k + \left\lfloor\left(\frac{3}{2}\right)^k\right\rfloor - 2$$

Theorem (Mahler, 1957). The equality holds for all but finitely many k .

Modern Waring's Problem. For $k \in \mathbb{N}$ with $k \geq 2$, let $G(k)$ denote the least integer $s = s(k)$ such that for all $n \in \mathbb{N}$ sufficiently large, there exist $x_1, \dots, x_s \in \mathbb{N}$ such that

$$n = x_1^k + x_2^k + \dots + x_s^k = \sum_{i=1}^s x_i^k$$

We know that $G(k) \leq g(k)$. Only known cases: $G(2) = 4$ and $G(4) = 16$.

Hardy-Littlewood (1920), Hua(1938). $G(k) \leq 2^k + 1$

The bound was improved by Vinogradov, Vaughan and others.

Theorem (Wooley, 1992). For large values of k , $G(k) \leq k(\log k + \log \log k + O(1))$.

Recently in 2022, the bound was improved drastically,

Theorem (Brudern & Wooley, 2022). For large values of k , $G(k) \leq k(\log k + O(1))$

We will introduce an important method by Hardy-Littlewood-Ramanujan that drastically revolutionized analytic number in last 100 years. This technique is called the circle method.

Fix $k, s \in \mathbb{N}$ with $k \geq 2$. For $n \in \mathbb{N}$, let

$$R(n) = R_{s,k}(n) = \left| \left\{ n = \sum_{i=1}^s x_i^k : x_i \in \mathbb{N} \right\} \right|$$

Note that $x_i \leq \sqrt[k]{n}$. For $\alpha \in \mathbb{R}$, let $e(\alpha) = 2^{2\pi i \alpha}$. For $m \in \mathbb{Z}$,

$$\int_0^1 e(\alpha m) d\alpha = \begin{cases} 1 & \text{if } m = 0 \\ 0 & \text{otherwise} \end{cases}$$

It follows that

$$\sum_{x_1 \leq \sqrt[k]{n}} \dots \sum_{x_s \leq \sqrt[k]{n}} \int_0^1 e\left(\alpha \left(\sum_{i=1}^s x_i^k - n\right)\right) d\alpha = R(n)$$

Idea. To estimate


$$\sum_{x \leq \sqrt[k]{n}} e(\alpha x^k)$$

we relate it to the geometric series

$$\sum_{x \leq \sqrt[k]{n}} e(\alpha x)$$

Weyl's Differencing, Consider

$$\left| \sum_{x \leq \sqrt[k]{n}} e(\alpha x^k) \right|^2 = \sum_{x \leq \sqrt[k]{n}} \sum_{(x+h) \leq \sqrt[k]{n}} e(\alpha((x+h)^k - x^k))$$

where $(x+h)^k - x^k$ is a polynomial of degree $(k-1)$ in x . After differencing $(k-1)$ -times, we get a linear polynomial (i.e., a geometric series) with leading coefficient $k!$. 

2. Analogies between \mathbb{Z} and $\mathbb{F}_p[t]$

We will first observe the generalized analogy between \mathbb{Z} and $\mathbb{F}[x]$, where $F[x]$ is a polynomial ring.

	\mathbb{Z}	$F[x]$
elements	m	$f(x)$
lowest factor	prime p	irreducible polynomial $h(x)$
size	$ m $	$\deg f$
units	$\{\pm 1\}$	F^\times (or F^*)
positive	$(\mathbb{Z} \setminus \{0\}) / \langle \pm 1 \rangle \cong \mathbb{N}$	$(F[x] \setminus \{0\}) / F^\times \cong \{\text{monic polynomials}\}$
unique factorization	$m = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, p_i prime	$f = cl_1^{\alpha_1} \cdots l_r^{\alpha_r}$, $l_i = l_i(t)$ monic, $c \in F^\times$
ideals	$\langle n \rangle$: unique if $n \in \mathbb{N}$	$\langle h(x) \rangle$: $h(x)$ is monic
quotient rings	$\mathbb{Z} / \langle n \rangle$ is a field $\iff n$ is prime	$F[x] / \langle h(x) \rangle$ is a field $\iff h(x)$ is irreducible.

Let \mathbb{Z} be the set of integers. We know that the set is closed under $+$ and \cdot and has a ring structure. We measure $n \in \mathbb{Z}$ by $|n|$. \mathbb{Z} is an integral domain and its fraction field is \mathbb{Q} . \mathbb{R} is the completion of \mathbb{Q} with respect to $|\cdot|$.

Let p be a prime and \mathbb{F}_p the finite field of p elements. Let

$$\mathbb{F}_p[t] = \left\{ \sum_{i=0}^n a_i t^i : n \in \mathbb{N} \cup \{0\} \text{ and } a_i \in \mathbb{F}_p \right\}$$

be the set of polynomials in t over \mathbb{F}_p . We know that the set is closed under $+$ and \cdot and has a ring structure. We measure $f(t) \in \mathbb{F}_p[t]$ by $\deg f$ or $\langle f \rangle = p^{\deg f}$. $\mathbb{F}_p[t]$ is an integral domain and its fraction field is $\mathbb{F}_p(t)$. $\mathbb{F}_p(\langle \frac{1}{t} \rangle)$ is the completion of $\mathbb{F}_p(t)$ with respect to $\langle \cdot \rangle$, where

$$\mathbb{F}_p \left(\left\langle \left(\frac{1}{t} \right) \right\rangle \right) = \left\{ \sum_{i \leq r} a_i t^i : a_i \in \mathbb{F}_p \right\}$$

We recall that for Fermat's last theorem, the equation

$$x^n + y^n = z^n \quad (n \geq 3)$$

involves both \cdot and $+$. Similarly, for Waring's problem, the equation

$$n = \sum_{i=1}^s x_i^k \quad (k \geq 2)$$

also uses both \cdot and $+$

Question. Fermat's last theorem and Waring's problem in $\mathbb{F}_p[t]$?

3. Fermat's Last Theorem in $\mathbb{F}_p[t]$

Let $n \in \mathbb{N}$ with $n \geq 3$. For $f(t), g(t), h(t) \in \mathbb{F}_p[t]$ with

$$f(t)^n + g(t)^n = h(t)^n$$

we say (f, g, h) is a non-trivial solution if $\deg(f), \deg(g), \deg(h)$ are ≥ 1 . We notice that for $f(t), g(t), h(t) \in \mathbb{F}_p[t]$,

$$f(t)^p + g(t)^p = (f(t) + g(t))^p = h(t)^p$$

where $h(t) = f(t) + g(t)$. Hence there are infinitely many non-trivial solutions.

Theorem (Fermat's Last Theorem in $\mathbb{F}_p[t]$). For $n \in \mathbb{N}$ with $n \geq 3$ and $\gcd(n, p) = 1$, the equation

$$f(t)^n + g(t)^n = h(t)^n$$

has no non-trivial solution in $\mathbb{F}_p[t]$.

Proof. Suppose that we have a non-trivial solution with $\gcd(f, g) = 1$ and $\deg(f) = \deg(h) \geq \deg(g)$. Differentiate the equation to get

$$n f^{n-1} f' + n g^{n-1} g' = n h^{n-1} h'$$

Since $\gcd(n, p) = 1$, by multiplying both sides by h ,

$$f^{n-1} f' h + g^{n-1} g' h = h^n h' = f^n h' + g^n h'$$

The last equality holds since $h^n = f^n + g^n$. So we have

$$f^{n-1} (f' h - f h') = g^{n-1} (g h' - g' h)$$

Since $\gcd(f, g) = 1$,

$$f^{n-1} \mid (g h' - g' h)$$

So,

$$(n - 1) \deg f \leq \deg g + \deg h - 1$$

Since $\deg h = \deg f$, we get

$$(n - 2) \deg f \leq \deg g - 1$$

Since $n \geq 3$, it follows that $\deg f < \deg g$, a contradiction. Hence, there is no non-trivial solution to $f^n + g^n = h^n$. □

4. Waring's Problem in $\mathbb{F}_p[t]$ Let $k \in \mathbb{N}$ with $k \geq 2$. We recall that $G(k)$ denotes the least integer $s = s(k)$ such that for all $n \in \mathbb{N}$ sufficiently large, there exists $x_1, \dots, x_s \in \mathbb{N}$ such that

$$n = \sum_{i=1}^s x_i^k$$

It is attempting to define $G_p(k)$ to be the least integer $s = s(k)$ such that for all $f(t) \in \mathbb{F}_p[t]$ with $\langle f \rangle$ sufficiently large, there exist $y_1(t), \dots, y_s(t) \in \mathbb{F}_p[t]$ such that

$$f(t) = \sum_{i=1}^s y_i(t)^k$$

Intrinsic obstructions exist in $\mathbb{F}_p[t]$. For example, $p \mid k$,

$$f(t) = \sum_{i=1}^s y_i(t)^k = \left(\sum_{i=1}^s y_i(t)^{\frac{k}{p}} \right)^p$$

So $f(t) \in \mathbb{F}_p[t^p]$, which is not the whole $\mathbb{F}_p[t]$. Let $\mathbb{J}_p^k[t]$ denote the additive closure of y^k with $y \in \mathbb{F}_p[t]$. Consider only $f \in \mathbb{J}_p^k[t]$ with $\langle f \rangle$ sufficiently large. Let

$$R_p(f) = \left| \left\{ f(t) = \sum_{i=1}^s y_i(t)^k : y_i(t) \in \mathbb{F}_p[t] \right\} \right|$$

We require $\langle y_i \rangle \leq \langle f \rangle^{\frac{1}{k}} \cdot c$, where $1 \leq c = c_{p,f} < p^2$.

We recall that the analogy of \mathbb{R} is $\mathbb{F}_p((1/t))$. One can define $e_p : \mathbb{F}_p((1/t)) \rightarrow \mathbb{C}$ such that for $h = h(t) \in \mathbb{F}_p[t]$,

$$\int_{\langle \beta \rangle < 1} e_p(\beta h) d\beta = \begin{cases} 1 & \text{if } h = 0 \\ 0 & \text{otherwise} \end{cases}$$

To estimate

$$\sum_{\langle y \rangle \leq c \langle f \rangle^{1/k}} e_p(\beta y^k)$$

we relate it to the geometric series

$$\sum_{\langle y \rangle \leq c(f)^{1/k}} e_p(\beta y)$$

by applying Weyl's differencing $(k - 1)$ -times. This gives us a degree 1 polynomial with leading coefficient $k!$. We get $k! = 0$ in $\mathbb{F}_p[t]$ if $k \geq p$ which isn't good!

Theorem (Kubota, 1971). If $k < p$, then $G_p(k) \leq 2^k + 1$.

Theorem (Car, Cherly, Gallardo). $G_2(3) \leq 10$.

Theorem (Wooley & L., 2010). If $k < p$, then $G_p(k) \leq k(\log k + \log \log k + O(1))$. If $k > p$ and $\gcd(k, p) = 1$, then $G_p(k) \leq Ck(\log k + \log \log k + O(1))$, where $1 \leq C = C_{k,p} \leq \frac{4}{3}$. If $p \mid k$, then $G_p(k) = G_p(k/p)$.

Idea. Use smooth polynomials and the large sieve inequality to replace Weyl's differencing. In order to get asymptotic estimates for smooth polynomials, we need to order polynomials one by one. One can use *refine ordering on* $\mathbb{F}_p[t]$. Consider the map: $\mathbb{F}_p[t] \rightarrow \mathbb{N} \cup \{0\}$ defined by

$$\sum_{i=0}^n a_i t^i \mapsto \sum_{i=0}^n a_i p^i$$

This ordering satisfies usual estimates for arithmetic progressions and asymptotic estimates for smooth polynomials. ✎

So, Result of Fermat vs Waring in terms of difficulties:

- In \mathbb{Z} , Fermat wins!
- In $\mathbb{F}_p[t]$, Waring wins!

5. Taylor Series in $\mathbb{F}_p[t]$

For $F(x) \in \mathbb{Z}[x]$ and $a \in \mathbb{Z}$, if we write

$$F(x) = \sum_{i=0}^{\infty} a_i (x - a)^i = a_0 + a_1(x - a) + a_2(x - a)^2 + \dots$$

then $a_0 = F(a)$, $a_1 = F'(a)$ and $a_2 = F^{(2)}(a)/2!$, ...

In general,

$$a_i = \frac{F^{(i)}(a)}{i!}$$

Question. For $G(x) \in (\mathbb{F}_p[t])[x]$ and $b \in \mathbb{F}_p[t]$, can we write

$$G(x) = \sum_{i=0}^{\infty} b_i (x - b)^i \quad \text{with} \quad b_i = \frac{G^{(i)}(b)}{i!}?$$

We have $i! = 0$ in $\mathbb{F}_p[t]$ if $i \geq p$, which is an issue.

6. Final Remarks

All of the above results hold with \mathbb{F}_p replaced by \mathbb{F}_q , where q is a power of p . How about $g_p(k)$, the least integer $s = s(k)$ such that for all $f(t) \in \mathbb{J}_p^k[t]$, there exist $y_1(t), \dots, y_s(t) \in \mathbb{F}_p[t]$ such that

$$f(t) = \sum_{i=1}^s y_i(t)^k$$

with $\langle y_i \rangle \leq c \sqrt[k]{\langle f \rangle}$? The problem is more difficult than $g(k)$.