Primitive root problems

Francesco Campagna

Basel University

08/11/2018

C. F. Gauss

Problem (Disquisitiones Arithmeticae, Art. 314):
Let $p \neq 2, 5$ be a prime number. How long is the period in the decimal expansion of $\frac{1}{p}$?

C. F. Gauss

Problem (Disquisitiones Arithmeticae, Art. 314):
Let $p \neq 2, 5$ be a prime number. How long is the period in the decimal expansion of $\frac{1}{p}$?

Example:

$$\frac{1}{7} = 0.\overline{142857}$$

C. F. Gauss

Problem (Disquisitiones Arithmeticae, Art. 314):
Let $p \neq 2, 5$ be a prime number. How long is the period in the decimal expansion of $\frac{1}{p}$?

Example:

$$\frac{1}{7} = 0.\overline{142857} \qquad \frac{1}{11} = 0.\overline{09}$$

Solution

$p \neq 2, 5 \Rightarrow 10 \pmod{p} \in \mathbb{F}_p^*$. Let k be the order of 10 modulo p.

Solution

$p \neq 2, 5 \Rightarrow 10 \pmod{p} \in \mathbb{F}_p^*$. Let k be the order of 10 modulo p.

$$10^k \equiv 1 \bmod p \Rightarrow \exists b \in \mathbb{N} : pb = 10^k - 1$$

Solution

$p \neq 2, 5 \Rightarrow 10 \pmod{p} \in \mathbb{F}_p^*$. Let k be the order of 10 modulo p.

$$10^k \equiv 1 \bmod p \Rightarrow \exists b \in \mathbb{N} : pb = 10^k - 1$$

Hence

$$\frac{1}{p} = \frac{b}{10^k - 1} = \frac{b \cdot 10^{-k}}{1 - 10^{-k}} = \sum_{j=1}^{\infty} b \cdot 10^{-jk}.$$

Solution

$p \neq 2, 5 \Rightarrow 10 \pmod{p} \in \mathbb{F}_p^*$. Let k be the order of 10 modulo p.

$$10^k \equiv 1 \bmod p \Rightarrow \exists b \in \mathbb{N} : pb = 10^k - 1$$

Hence

$$\frac{1}{p} = \frac{b}{10^k - 1} = \frac{b \cdot 10^{-k}}{1 - 10^{-k}} = \sum_{j=1}^{\infty} b \cdot 10^{-jk}.$$

So k is greater or equal to the the length of the period of $\frac{1}{p}$. By reversing the argument one sees that in fact equality holds.

Solution

$p \neq 2,5 \Rightarrow 10 \pmod{p} \in \mathbb{F}_p^*$. Let k be the order of 10 modulo p.

$$10^k \equiv 1 \bmod p \Rightarrow \exists b \in \mathbb{N} : pb = 10^k - 1$$

Hence

$$\frac{1}{p} = \frac{b}{10^k - 1} = \frac{b \cdot 10^{-k}}{1 - 10^{-k}} = \sum_{j=1}^{\infty} b \cdot 10^{-jk}.$$

So k is greater or equal to the the length of the period of $\frac{1}{p}$. By reversing the argument one sees that in fact equality holds.

Answer: The length of the period of $\frac{1}{p}$ is the order of 10 mod p.

For instance:

$$\mathrm{ord}_{\mathbb{F}_7^*}(10) = 6 \qquad \mathrm{ord}_{\mathbb{F}_{11}^*}(10) = 2$$

For instance:

$$\mathrm{ord}_{\mathbb{F}_7^*}(10) = 6 \qquad \mathrm{ord}_{\mathbb{F}_{11}^*}(10) = 2$$

In particular if 10 mod p generates $\mathbb{F}_p^*$, the length of the period of $\frac{1}{p}$ is maximal ($= p - 1$).

For instance:

$$\mathrm{ord}_{\mathbb{F}_7^*}(10) = 6 \qquad \mathrm{ord}_{\mathbb{F}_{11}^*}(10) = 2$$

In particular if 10 mod p generates $\mathbb{F}_p^*$, the length of the period of $\frac{1}{p}$ is maximal $(= p - 1)$.

Definition

Let a be an integer. We say that a is a primitive root modulo p if a mod p generates $\mathbb{F}_p^*$, i.e. $\langle a \bmod p \rangle = \mathbb{F}_p^*$.

For instance:

$$\mathrm{ord}_{\mathbb{F}_7^*}(10) = 6 \qquad \mathrm{ord}_{\mathbb{F}_{11}^*}(10) = 2$$

In particular if 10 mod p generates $\mathbb{F}_p^*$, the length of the period of $\frac{1}{p}$ is maximal $(= p - 1)$.

Definition

Let a be an integer. We say that a is a primitive root modulo p if a mod p generates $\mathbb{F}_p^*$, i.e. $\langle a \bmod p \rangle = \mathbb{F}_p^*$.

Question

Let $a \neq \pm 1$ be a non-zero integer. For how many primes p is a a primitive root modulo p?

Some experiments

We consider all the primes up to 10^6.

a	**"primitive root" primes**	**Fraction**

Some experiments

We consider all the primes up to 10^6.

a	**"primitive root" primes**	**Fraction**
2	29341	0.3737

Some experiments

We consider all the primes up to 10^6.

a	**"primitive root" primes**	**Fraction**
2	29341	0.3737
3	29393	0.3744

Some experiments

We consider all the primes up to 10^6.

a	**"primitive root" primes**	**Fraction**
2	29341	0.3737
3	29393	0.3744
4	0	0

Some experiments

We consider all the primes up to 10^6.

a	"primitive root" primes	Fraction
2	29341	0.3737
3	29393	0.3744
4	0	0
5	30885	0.3934
6	29348	0.3739
7	29434	0.3749
8	17623	0.2245
9	1	0.0000
10	29500	0.3758
11	29433	0.3749

Natural densities

Definition

Let S be a subset of prime numbers. If the limit

$$\delta(S) := \lim_{x \to \infty} \frac{\#\{p \in S : p \leq x\}}{\#\{p \in \mathbb{Z} : p \leq x\}}$$

exists, then we call $\delta(S)$ the natural density of S.

Natural densities

Definition

Let S be a subset of prime numbers. If the limit

$$\delta(S) := \lim_{x \to \infty} \frac{\#\{p \in S : p \leq x\}}{\#\{p \in \mathbb{Z} : p \leq x\}}$$

exists, then we call $\delta(S)$ the natural density of S.

Example 1: If S is a finite set then $\delta(S) = 0$.

Natural densities

Definition

Let S be a subset of prime numbers. If the limit

$$\delta(S) := \lim_{x\to\infty} \frac{\#\{p \in S : p \leq x\}}{\#\{p \in \mathbb{Z} : p \leq x\}}$$

exists, then we call $\delta(S)$ the natural density of S.

Example 1: If S is a finite set then $\delta(S) = 0$.
Example 2: If q is a prime number and

$$S = \{p \text{ prime} : \; p \equiv 1 \bmod q\}$$

then $\delta(S) = \frac{1}{q-1}$.

Artin's primitive root conjecture

Artin's problem

Fix a non-zero integer $a \neq \pm 1$. What is the density of the set of primes p for which a is a primitive root modulo p?

Artin's primitive root conjecture

Artin's problem

Fix a non-zero integer $a \neq \pm 1$. What is the density of the set of primes p for which a is a primitive root modulo p?

Artin's conjecture: Let $a \neq \pm 1$ be a non-zero integer that is not a square. Then there exist infinitely many primes p for which a is a primitive root modulo p. Moreover if we write $a = b^n$ with $b \in \mathbb{Z}$ not a perfect power then the density $A(a)$ exists and its value is

$$A(a) = \prod_{l \nmid n} \left(1 - \frac{1}{l(l-1)}\right) \prod_{l \mid n} \left(1 - \frac{1}{l-1}\right).$$

Why?

What does it mean for an integer a to be a primitive root mod p?
Assume $p \nmid 2a$:

Why?

What does it mean for an integer a to be a primitive root mod p? Assume $p \nmid 2a$:

$$\langle a \bmod p \rangle = \mathbb{F}_p^* \iff a^{\frac{p-1}{l}} \not\equiv 1 \pmod{p} \text{ for any prime } l$$

$$\iff \begin{cases} p \equiv 1 \pmod{l} \\ a^{\frac{p-1}{l}} \equiv 1 \pmod{p} \end{cases} \text{don't occur for any prime } l$$

Why?

What does it mean for an integer a to be a primitive root mod p? Assume $p \nmid 2a$:

$$\langle a \bmod p\rangle = \mathbb{F}_p^* \iff a^{\frac{p-1}{l}} \not\equiv 1 \pmod{p} \text{ for any prime } l$$

$$\iff \begin{cases} p \equiv 1 \pmod{l} \\ a^{\frac{p-1}{l}} \equiv 1 \pmod{p} \end{cases} \text{don't occur for any prime } l$$

The last condition is equivalent to p not splitting completely in any $F_l := \mathbb{Q}(\zeta_l, \sqrt[l]{a})$ for any l prime.

By Chebotarev Density Theorem the density of the primes that do not split completely in F_l is $1 - \frac{1}{[F_l:\mathbb{Q}]}$.

By Chebotarev Density Theorem the density of the primes that do not split completely in F_l is $1 - \frac{1}{[F_l:\mathbb{Q}]}$.

$$[F_l : \mathbb{Q}] = \begin{cases} l(l-1) & \text{if } a \text{ is not an } l\text{-th power in } \mathbb{Q} \\ l-1 & \text{otherwise} \end{cases}$$

By Chebotarev Density Theorem the density of the primes that do not split completely in F_l is $1 - \frac{1}{[F_l:\mathbb{Q}]}$.

$$[F_l : \mathbb{Q}] = \begin{cases} l(l-1) & \text{if } a \text{ is not an } l\text{-th power in } \mathbb{Q} \\ l-1 & \text{otherwise} \end{cases}$$

If we assume the splitting conditions all independent we recover the formula

$$\prod_{l \nmid n} \left(1 - \frac{1}{l(l-1)}\right) \prod_{l \mid n} \left(1 - \frac{1}{l-1}\right)$$

Theorem (Hooley)

Assuming the Generalized Riemann Hypothesis, the density of the set of primes p for which a given integer a is a primitive root modulo p equals

$$\delta(a) = \sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(\sqrt[m]{a}, \zeta_m) : \mathbb{Q}]}.$$

Moreover when $\operatorname{disc}(\mathbb{Q}(\sqrt{a})/\mathbb{Q}) \not\equiv 1 \bmod 4$*, this density has the product factorization*

$$\delta(a) = \prod_{l \nmid n} \left(1 - \frac{1}{l(l-1)}\right) \prod_{l \mid n} \left(1 - \frac{1}{l-1}\right)$$

Elliptic curves analogues

Let E be an elliptic curve defined over a number field $\mathbb{Q}$:

$$E : y^2 = x^3 + Ax + B \qquad A, B \in \mathbb{Z}$$

with $\Delta_E = -16(4A^3 + 27B^2) \neq 0$.

Elliptic curves analogues

Let E be an elliptic curve defined over a number field $\mathbb{Q}$:

$$E : y^2 = x^3 + Ax + B \qquad A, B \in \mathbb{Z}$$

with $\Delta_E = -16(4A^3 + 27B^2) \neq 0$.

For every prime p in $\mathbb{Q}$ we can reduce E modulo p $\rightsquigarrow$ $\tilde{E}/\mathbb{F}_p$.

Elliptic curves analogues

Let E be an elliptic curve defined over a number field $\mathbb{Q}$:

$$E : y^2 = x^3 + Ax + B \qquad A, B \in \mathbb{Z}$$

with $\Delta_E = -16(4A^3 + 27B^2) \neq 0$.

For every prime p in $\mathbb{Q}$ we can reduce E modulo p $\rightsquigarrow$ $\tilde{E}/\mathbb{F}_p$.

- For p of bad reduction (dividing Δ_E) $\rightsquigarrow$ $\tilde{E}/\mathbb{F}_p$ is singular.

Elliptic curves analogues

Let E be an elliptic curve defined over a number field $\mathbb{Q}$:

$$E : y^2 = x^3 + Ax + B \qquad A, B \in \mathbb{Z}$$

with $\Delta_E = -16(4A^3 + 27B^2) \neq 0$.

For every prime p in $\mathbb{Q}$ we can reduce E modulo $p \rightsquigarrow \tilde{E}/\mathbb{F}_p$.

- For p of bad reduction (dividing Δ_E) $\rightsquigarrow \tilde{E}/\mathbb{F}_p$ is singular.
- For p of good reduction $\rightsquigarrow \tilde{E}/\mathbb{F}_p$ is an elliptic curve.

Elliptic curves analogues

Let E be an elliptic curve defined over a number field $\mathbb{Q}$:

$$E : y^2 = x^3 + Ax + B \qquad A, B \in \mathbb{Z}$$

with $\Delta_E = -16(4A^3 + 27B^2) \neq 0$.

For every prime p in $\mathbb{Q}$ we can reduce E modulo p $\rightsquigarrow$ $\tilde{E}/\mathbb{F}_p$.

- For p of bad reduction (dividing Δ_E) $\rightsquigarrow$ $\tilde{E}/\mathbb{F}_p$ is singular.
- For p of good reduction $\rightsquigarrow$ $\tilde{E}/\mathbb{F}_p$ is an elliptic curve.

$$\text{The group } \tilde{E}(\mathbb{F}_p) = \begin{cases} \text{cyclic} \\ \text{product of two cyclic groups} \end{cases}$$

Elliptic curves analogues

Immediate elliptic curve analogue of Artin's primitive root problem:

Problem: Let E be an elliptic curve defined over $\mathbb{Q}$ and let $R \in E(\mathbb{Q})$ be a point of infinite order. What is the density of the set of primes p such that $\tilde{E}(\mathbb{F}_p)$ is cyclic, generated by the reduction of R modulo p?

Elliptic curves analogues

Immediate elliptic curve analogue of Artin's primitive root problem:

Problem: Let E be an elliptic curve defined over $\mathbb{Q}$ and let $R \in E(\mathbb{Q})$ be a point of infinite order. What is the density of the set of primes p such that $\tilde{E}(\mathbb{F}_p)$ is cyclic, generated by the reduction of R modulo p?

We call in this case R a **primitive point** mod p.

Elliptic curves analogues

Immediate elliptic curve analogue of Artin's primitive root problem:

Problem: Let E be an elliptic curve defined over $\mathbb{Q}$ and let $R \in E(\mathbb{Q})$ be a point of infinite order. What is the density of the set of primes p such that $\tilde{E}(\mathbb{F}_p)$ is cyclic, generated by the reduction of R modulo p?

We call in this case R a **primitive point** mod p.

Conjecture (Lang-Trotter)

The density of the set of primes for which R is a primitive point always exist.

Simpler problem:

What is the density of the primes of good reduction for which $\tilde{E}(\mathbb{F}_p)$ is cyclic?

Simpler problem:

What is the density of the primes of good reduction for which $\tilde{E}(\mathbb{F}_p)$ is cyclic?

Equation for E	**Primes up to 10^6 of cyclic reduction for E**	$d(E)$
$y^2 = x^3 - 19x + 30$	0	0
$y^2 = x^3 - 3x + 1$	49024	0.6510
$y^2 = x^3 + 2x + 3$	38383	0.4889
$y^2 = x^3 - 12096x - 544752$	32652	0.4159
$y^2 = x^3 + x + 3$	63910	0.8141
$y^2 = x^3 - 1$	39265	0.5002

Cyclic reduction problem

The cyclic reduction problem can be tackled in the same way as Artin's primitive root problem!

Cyclic reduction problem

The cyclic reduction problem can be tackled in the same way as Artin's primitive root problem!

If $E/\mathbb{Q}$ is an elliptic curve

$$E[m](\overline{\mathbb{Q}}) = \{P = (x, y) \in E(\overline{\mathbb{Q}}) : mP = O\} \cup \{O\}$$

Cyclic reduction problem

The cyclic reduction problem can be tackled in the same way as Artin's primitive root problem!

If $E/\mathbb{Q}$ is an elliptic curve

$$E[m](\overline{\mathbb{Q}}) = \{P = (x, y) \in E(\overline{\mathbb{Q}}) : mP = O\} \cup \{O\}$$

Definition

For $E/\mathbb{Q}$ an elliptic curve and $m \in \mathbb{N}$ the *m*-**division field** over $\mathbb{Q}$ is

$$K_m := \mathbb{Q}(E[m](\overline{\mathbb{Q}}))$$

Cyclic reduction problem

Proposition

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime of good reduction. Then $\tilde{E}(\mathbb{F}_p)$ is cyclic if and only if p does not split completely in any division field K_l with l prime.

Cyclic reduction problem

Proposition

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime of good reduction. Then $\tilde{E}(\mathbb{F}_p)$ is cyclic if and only if p does not split completely in any division field K_l with l prime.

$$\delta(\{p \text{ prime}: \ p \text{ does not split completely in } K_l, \ l \text{ prime}\})$$
$$||$$
$$\delta(\{p \text{ prime}: \tilde{E}(\mathbb{F}_p) \text{ is cyclic}\})$$

Cyclic reduction problem

Theorem (Serre)

Let E be an elliptic curve defined over $\mathbb{Q}$ and let

$$S = \{p \text{ prime}: \ \tilde{E}(\mathbb{F}_p) \text{ is cyclic}\}.$$

Then, subject to GRH, the density of S equals

$$\delta(E) = \sum_{m=1}^{\infty} \frac{\mu(m)}{[K_m : \mathbb{Q}]}$$

with μ the Möbius function and K_m the m-division field of E over $\mathbb{Q}$.

Thanks for your attention