On the introductory notes on Artin's Conjecture

The purpose of this note is to make the surveys [5] and [6] more accessible to bachelor students. We provide some further preliminaries and some exercises. We also present the calculations which lead to the density appearing in Hooley's formulas and a proof for the corollaries of the result by Heath-Brown.

Contents

1. What we are speaking about 1
2. The cyclicity of the group $(\mathbb{Z}/p\mathbb{Z})^*$ 1
3. Exercises on primitive roots 2
4. The modified density of Hooley's formulas 3
5. Corollaries of the result by Heath-Brown 5
6. Datas 5
References 6

1. What we are speaking about

One of the most famous open conjectures in number theory is Artin's primitive root conjecture, which is due to Emil Artin and dates back to 1927.

Let p denote a prime number and consider the reduction of the integers modulo p, so the ring homomorphism

$$\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$

which sends any integer to its residue class modulo p.
Let a be an integer not divisible by p. Then Fermat's Little Theorem tells us that

$$a^{p-1} \equiv 1 \pmod{p}.$$

This means that the integer $a^{p-1} - 1$ is divisible by p. Do there exist infinitely many primes p such that the smallest n such that

$$a^n \equiv 1 \pmod{p}$$

is in fact $p - 1$?
The classical version of Artin's primitive root conjecture states that the answer to this question is affirmative, provided that a is not a perfect square or -1.

2. The cyclicity of the group $(\mathbb{Z}/p\mathbb{Z})^*$

The set of non-zero residue classes modulo p is a group for the multiplication induced by $\mathbb{Z}/p\mathbb{Z}$. It is denoted by $(\mathbb{Z}/p\mathbb{Z})^*$. I outline two proofs of the fact that the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

Lemma 2.1. *A polynomial of degree d with coefficients in a field can have at most d distinct solutions.*

Proof. Let α be a solution for $f(x)$. Then we can write $f(x) = g(x)(x - \alpha) + r$ by euclidean division and the constant r is 0 (evaluate $f(\alpha)$). So $f(x) = g(x)(x - \alpha)$. A solution β of f is such that either $g(\beta) = 0$ or $(\beta - \alpha) = 0$. So if $\beta \neq \alpha$ then β is a solution of g and (by induction on the degree) there are at most $d - 1$ solutions for g. □

Lemma 2.2. *For the Euler-ϕ function, the following relation holds for every $n \geq 1$:*

$$n = \sum_{d|n} \phi(n)$$

Proof. One can prove the formula by induction on the number of prime factors of n. See [3, Proposition 2.2.4] □

For any group, the order of the sum of two elements clearly divides the least common multiple of the orders of the elements.

Lemma 2.3. *In a group, if two elements have orders which are coprime, then the order of the sum is exactly the product of the orders.*

Proof. Suppose that a and b have order n and m respectively and $(n, m) = 1$. Let $d \mid n$, $d \neq 1$. Then $\frac{nm}{d}(a \oplus b) = \frac{n}{d}(a) \neq 0$ hence the order does not divide $\frac{nm}{d}$ hence the order is a multiple of n (analogously for m). □

We know that the order of the group $(\mathbb{Z}/p\mathbb{Z})^*$ is $p-1$ hence it suffices to show that there is at least one element of order exactly $p-1$.

First proof
We first prove that there are at most $\phi(d)$ elements of order d. Suppose that there is an element a of order d. Then the powers $a, a^2 \ldots, a^d = 1$ are all distinct. They are d distinct solutions of the polynomial $x^d - 1$ so they are *all* the solutions of that polynomial. Thus every element which has order d, being a solution of $x^d - 1$, is a power of a. The order of the power of an element is given by the formula:

$$\operatorname{ord}(a^h) = \frac{\operatorname{ord}(a)}{(h, \operatorname{ord}(a))}$$

Then the powers of a whose order is d correspond to the integers $0 < h < d$ that are coprime to d: they are exactly $\phi(d)$. So we have shown that if there is an element of order d, there are exactly $\phi(d)$ such elements.
We have a set of $p-1$ elements, which is the disjoint union, for $d \mid p-1$, of subsets of order at most $\phi(d)$. Since

$$p - 1 = \sum_{d|p-1} \phi(d)$$

then it must be that every such subset has order $\phi(d)$. In particular, we have proven that for every $d \mid p-1$ (including $p-1$, which is what we need) there are exactly $\phi(d)$ elements of order d.

Second proof
Write $p-1$ as product of prime powers $p_i^{e_i}$. By Lemma 2.3, it suffices to find, for every i, an element which has order a multiple of $p_i^{e_i}$ (notice that a power of it will have order exactly $p_i^{e_i}$). Without loss of generality, suppose that no element has order a multiple of $p_1^{e_1}$, equivalently that every element has order dividing $\frac{p-1}{p_1}$. Then there would be $p-1$ distinct solutions of the polynomial $x^{\frac{p-1}{p_1}} - 1$, which has degree strictly smaller than $p-1$. Contradiction.

3. Exercises on primitive roots

(1) Prove that (2 mod 29) is a primitive root.
Hint: minimize your calculations by thinking of the group structure.

(2) List all the primitive roots modulo 19.
Hint: minimize your calculations by thinking of the group structure; you will possibly encounter the same elements when you do the calculations, so keep track of the informations you have already found.

(3) Prove that (a mod p) and its inverse [(b mod p) such that (ab mod p)= (1 mod p)] have the same order.

(4) Let q be a prime and define ord_q(a mod p) as the highest power of q dividing the order of (a mod p). Show that if ord_q(a mod p)>ord_q(b mod p) then ord_q(ab mod p)=ord_q(a mod p).

(5) Let p be an odd prime.
Prove that (a mod p) and (-a mod p) have the same order if 4 divides the order of (a mod p).
Prove that (-a mod p) has order twice the order of (a mod p), if the order of (a mod p) is odd.
Prove that the order of (-a mod p) is half of the order of (a mod p), if the order of (a mod p) is even but not divisible by 4.
Hint: Use exercise 4. Show that ord_q(a mod p)=ord_q(-a mod p) for every odd prime q hence restrict your attention to ord_2. For the last assertion, consider that if you raise (a mod p) to the

odd part of its order, you must necessarily get (-1 mod p) [which is the only element of order 2].

(6) Let G be a finite group and let g be an element of G. Show that the order of $n \cdot g$ is $\frac{ord(g)}{(ord(g),n)}$.
Hint: write $n = (ord(g), n) \cdot n'$, with $(ord(g), n')$=1.

(7) Let d be a divisor of $p-1$. Let (g mod p) be a primitive root. Show that ($g^{p-1/d}$ mod p) has order exactly d.
Hint: use exercise 6.

(8) Let p be an odd prime. Show that (a mod p) is a primitive root modulo p if and only if ($a^{p-1/d}$ mod p) is not (1 mod p), for every prime divisor d of $p-1$.
Hint: use exercise 7.

(9) Show that the d-th powers [(a mod p)=(b^d mod p) for some b] form a subgroup. Show that if $d \mid (p-1)$ then the order of this subgroup is $(p-1)/d$. Show that if $(p-1, d) = 1$ then every element is a d-th power.
Hint: Let (g mod p) be a primitive root. Then show that (a mod p) is a d-th power if and only if one can write (a mod p)=(g^{dk} mod p) for some integer k. For the last assertion, use the fact that d has an inverse d' modulo $(p-1)$, hence (g^k mod p)=($g^{d(d'k)}$ mod p) for every integer k.

(10) Show that there are $\phi(p-1)$ primitive roots. Let a be as in Artin's conjecture, and not a power. Prove that if $p > 3$ the expected probability that (a mod p) is a primitive root is at most $1 - \frac{1}{\sqrt{p-1}}$. Check that this is the expected probability if $p - 1 = q^2$, where q is prime. [For p=2,3 the values are 1 and 1/2 respectively.]

(11) Explain why we exclude 0, ± 1 and squares from Artin's conjecture. Explain also why a priori we do not exclude other powers.
Hint: 2 divides $p-1$ for every odd prime; see the hint of exercise 9. Recall Dirichlet's theorem on primes in arithmetic progression to argument that there are 'many' primes for which $p-1$ is not divisible by some fixed odd number.

4. The modified density of Hooley's formulas

In this section, I show how one arrives from Artin's heuristics to the formula of the density which appears in Hooley's result. This calculation is taken from [2, Section 6]. Following Artin's heuristics, to calculate the density we simply have to evaluate:

$$\sum_{n\, squarefree} \frac{\mu(n)}{[K_n : \mathbb{Q}]}$$

where μ is the Moebius function and K_n is the compositum of $\mathbb{Q}(\zeta_q, a^{1/q})$ for every prime number q which divides n. So we are taking a sum of the inverses of the degrees over $\mathbb{Q}$ of the number fields K_n (with a sign $\pm$ according to the Moebius function).

Euler products. Let $a(n)$ be a function defined over the natural numbers ($n > 0$) which is multiplicative, which means $a(1) = 1$ and $a(mn) = a(m)a(n)$ whenever m, n are coprime. Then the Euler product formula says:

$$\sum_n a(n) = \prod_p \Big(1 + a(p) + a(p^2) + \cdots\Big)$$

If $a(n) = 0$ for n not squarefree then the following simplified version clearly holds:

$$\sum_{n\, squarefree} a(n) = \sum_n a(n) = \prod_p \Big(1 + a(p) + a(p^2) + \cdots\Big) = \prod_p \Big(1 + a(p)\Big)$$

The case of linear disjoint extensions. Suppose that we are in the case where the extensions $\mathbb{Q}(\zeta_q, a^{1/q})$ are linearly disjoint for every prime number q (so, including $q = 2$). This means that $a = bc^2$ for some

integers b, c and that $b \not\equiv 1 \pmod 4$. We are then in the case where

$$[K_n : \mathbb{Q}] = \frac{n\phi(n)}{(h,n)}$$

where h is the biggest integer such that a has an h-th root in the integers. The requested density is then

$$\sum_{n\, squarefree} \frac{\mu(n)}{[K_n : \mathbb{Q}]} = \prod_p \Big(1 + \frac{\mu(p)}{[K_p : \mathbb{Q}]}\Big) = \prod_{p|h} \Big(1 - \frac{p}{p(p-1)}\Big) \prod_{p\nmid h} \Big(1 - \frac{1}{p(p-1)}\Big) = A(h)$$

The number $A(h)$ is obviously a rational multiple of Artin's constant

$$A = \prod_p \Big(1 - \frac{1}{p(p-1)}\Big)$$

The case of non-linear disjoint extensions. Suppose that $a = bc^2$ for some integers b, c and that $b \equiv 1 \pmod 4$. In particular, b is odd. Then

$$[K_n : \mathbb{Q}] = \begin{cases} \frac{n\phi(n)}{2(h,n)} & \text{if } n \text{ is even and } b \mid n \\ \\ \frac{n\phi(n)}{(h,n)} & \text{otherwise} \end{cases}$$

where h is the biggest integer such that a has an h-th root in the integers. Recall that h is odd since we exclude squares from Artin's conjecture.
We have:

$$\sum_n \frac{\mu(n)}{[K_n : \mathbb{Q}]} = \sum_{n \not\equiv 0 (\text{mod } 2|b|)} \frac{\mu(n)(h,n)}{n\phi(n)} + 2 \cdot \sum_{n \equiv 0 (\text{mod } 2|b|)} \frac{\mu(n)(h,n)}{n\phi(n)} = A(h) + \sum_{n \equiv 0 (\text{mod } 2|b|)} \frac{\mu(n)(h,n)}{n\phi(n)}$$

If m is squarefree and $m \equiv 0 \pmod{2|b|}$ we can write $m = 2|b|n$ with n coprime to $2|b|$. Then we have:

$$\sum_{n \equiv 0 (2|b|)} \frac{\mu(n)(h,n)}{n\phi(n)} = \sum_{n:(n,2|b|)=1} \frac{\mu(2|b|n)(h,2|b|n)}{(2|b|n)\phi(2|b|n)} = \frac{\mu(2|b|)(h,2|b|)}{(2|b|)\phi(2|b|)} \cdot \sum_{n:(n,2|b|)=1} \frac{\mu(n)(h,n)}{n\phi(n)}$$

Let $\tilde{\mu}(n)$ be equal to $\mu(n)$ whenever $(n, 2|b|) = 1$ and equal to 0 otherwise. By taking the Euler product we get:

$$\sum_n \frac{\tilde{\mu}(n)(h,n)}{n\phi(n)} = \prod_p \Big(1 + \frac{\tilde{\mu}(p)(h,p)}{p\phi(p)}\Big) = \prod_{p:\, p\nmid(2|b|)} \Big(1 + \frac{\mu(p)(h,p)}{p\phi(p)}\Big) = \prod_{p:\, p\nmid(2|b|)} \Big(1 - \frac{(h,p)}{p\phi(p)}\Big) =$$

$$A(h) \cdot \prod_{p:\, p|(2|b|)} \Big(1 - \frac{(h,p)}{p\phi(p)}\Big)^{-1} = A(h) \cdot \prod_{p:\, p|(2|b|)} \frac{p\phi(p)}{p\phi(p) - (h,p)}$$

Putting things together:

$$\sum_n \frac{\mu(n)}{[K_n : \mathbb{Q}]} = A(h)\Big[1 + \frac{\mu(2|b|)(h,2|b|)}{2|b|\phi(2|b|)} \cdot \prod_{p:\, p|(2|b|)} \frac{p\phi(p)}{p\phi(p) - (h,p)}\Big] =$$

$$= A(h)\Big[1 - \mu(|b|)(h,2|b|) \cdot \prod_{p:\, p|(2|b|)} \frac{1}{p\phi(p) - (h,p)}\Big] = A(h)\Big[1 - \mu(|b|) \cdot \prod_{p:\, p|(2|b|)} \frac{(h,p)}{p\phi(p) - (h,p)}\Big] =$$

$$= A(h)\Big[1 - \mu(|b|) \cdot \prod_{p:\, p|b; p|h} \frac{1}{\phi(p) - 1} \cdot \prod_{p:\, p|b; p\nmid h} \frac{1}{p\phi(p) - 1}\Big] = A(h)\Big[1 - \mu(|b|) \cdot \prod_{p|b} \frac{1}{[K_p : \mathbb{Q}] - 1}\Big]$$

5. Corollaries of the result by Heath-Brown

An n-tuple of integer numbers $x_1, \dots, x_n$ is said to be multiplicative dependent (the numbers are then called multiplicative dependent) if there exist $a_1, \dots, a_n$ integers, not all zero, such that $\prod_1^n x_i^{a_i} = 1$. *Multiplicative independent* means not multiplicatively dependent in the sense above.

Heath-Brown proved in 1967 ([1]) the following result:

Theorem 5.1. *If q, r, s are three nonzero multiplicatively independent integers such that none of*

$$q, r, s, -3qr, -3qs, -3rs, qrs$$

is a square, then there are infinitely many prime numbers p for which at least one between q, r, s is a primitive root modulo p.

We deduce the following:

Corollary 5.2. *Consider the classical version of Artin's conjecture (we look for an infinite set of primes p):*

(1) There are at most two prime numbers for which Artin's conjecture fails.
(2) There are at most three positive squarefree numbers ($\neq 1$) for which Artin's conjecture fails.

Lemma 5.3. *Let x, y, z be three distinct positive squarefree integers ($\neq 1$) and suppose that $x^a y^b z^c = 1$ for some integers a, b, c. Then (up to a reordering) we have $z = xy$ and $(x, y) = 1$.*

Proof. It is easy to see that one or two distinct positive squarefree integers ($\neq 1$) are always multiplicative independent. Then a, b, c are all non-zero. Since x, y, z are integers, a, b, c cannot be all > 0 or all < 0. So, without loss of generality, we can write $x^a y^b = z^c$ for some $a, b, c > 0$.
Since x and y are distinct squarefree integers there exists p prime (w.l.o.g.) dividing x but not y. Hence c must divide a (the left-hand side is a c-th power). So we have $x^{ca'} y^b = z^c$. By comparing the exponents in the prime factorisations, $c \mid b$.
Then we have $x^{a'} y^{b'} = z$ [we could have $x^{a'} \zeta_c^n \cdot y^{b'} \zeta_c^m = z$ but since x, y, z are positive integers it must be that $\zeta_c^n \zeta_c^m$ is also a positive integer, hence it is 1]. So we have $x^{a'} y^{b'} = z$. Since $a' > 0$, $b' > 0$ and z is square-free it follows that $a' = b' = 1$ and $(x, y) = 1$. So $z = xy$ and $(x, y) = 1$. □

Proof of Corollary 5.2. (1) Suppose that there are three distinct prime numbers q, r, s for which Artin's conjecture fails. They are multiplicative independent and qrs is not a square. Since negative numbers are not squares, we apply the result by Heath-Brown and deduce a contradiction.
(2) It suffices to show that in every set of four distinct positive squarefree integers ($\neq 1$), there is at least one which satisfies Artin's conjecture. We will show that for every four distinct positive squarefree integers ($\neq 1$), there are three of them which are multiplicatively independent and are such that the product of them is not a square. It is then clear (since negative integers are never squares) that the assumptions of the result of Heath-Brown hold. Hence at least one of the four numbers satisfies Artin's conjecture.
Let $\{x, y, z, w\}$ be our set of four distinct positive squarefree integers ($\neq 1$). First case: there are three elements in our set which are dependent. So w.l.o.g. we have $z = xy$ and $(x, y) = 1$. Since $w \neq xy$ and $(x, y) = 1$ [hence $x \nmid y$ or viceversa] Lemma 5.3 implies that $\{x, y, w\}$ are independent. We have that xyw is not a square: since $(x, y) = 1$ and w is squarefree, that would imply $w = xy$.
Second case: no three elements in our set are dependent. What if xyz is a square? Let $\delta = (x, y)$ so that $x = \delta x'$ and $y = \delta y'$. Because z is square-free then that would imply $z = x'y'$. Since $w \neq z$ we then conclude that xyw is not a square. □

In particular, Artin's conjecture is true for at least one in between 2,3,5.

6. Datas

I collect some datas which are available at The On-Line Encyclopedia of Integer Sequences (OEIS).

Datas for $(2 \bmod p)$*:*
The primes p up to 1.000 for which $(2 \bmod p)$ is a primitive root, see:
http://oeis.org/classic/A001122

(PARI) forprime(p=3, 1000, if(znprimroot(p)==2, print(p))).

3,5,11,13,19,29,37,53,59,61,67,83,101,107,131, 139,149,163,173,179,181,197,211,227,269,293,317,
347,349,373,379,389,419,421,443,461,467,491,509, 523,541,547,557,563,587,613,619,653,659,661,677,
701,709,757,773,787,797

Let a(n) be the n-th term of the sequence above. There is a graphic for (n, a(n)) at the page: http://oeis.org/classic/table?a=1122&fmt=5
This graphic visually shows the density of the set of primes p such that (2 mod p) is a primitive root.

Artin's constant:
You can look at the first cyphers of the decimal expansion of Artin's constant (with graphic), by following the links at the page: http://oeis.org/classic/A005596

Datas for other elements:
Unfortunately, the program

(PARI) forprime(p=3, 1000, if(znprimroot(p)==3, print(p))).

seems to print the primes for which 3 is the smallest primitive root, so it excludes those for which both 2 and 3 are primitive roots. See http://oeis.org/classic/A001123
But for any a we can write:

(PARI) if(znorder(Mod(a,p))==p-1, print(p)).

For 6, see: http://oeis.org/classic/A019336
You get the list of primes for which 6 is a primitive root:

(MATEMATICA) pr=6; Select[Prime[Range[200]], MultiplicativeOrder[pr, #] == #-1 &]

By replacing 6 with 8, see: http://oeis.org/classic/A019338
The same program line command with (MATEMATICA), by replacing 6 by 3, should give you the primes (between the first 200 primes) such that (3 mod p) is a primitive root.

Possible computational exercises:

- Study the reductions modulo the first rational primes (200 primes, or primes up to 1000) and compare the (approximated) densities for a=2 with the approximated Artin's constant [decimal expansion].
- Study the reductions modulo the first rational primes (200 primes, or primes up to 1000) and compare the (approximated) densities for a=8 with the modified Artin's constant $A(3)$ [you can deduce the decimal expansion of $A(3)$ from that of A].

References

[1] D. R. Heath-Brown, *Artins conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38.
[2] C. Hooley, *On Artins conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.
[3] K. Ireland and M. Rosen, *A classical Introduction to modern number theory*, Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990. xiv+389 pp.
[4] S. Lang, *Algebra*, Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002. xvi+914 pp.
[5] R. Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer **10** (1988) no. 4, 59–67, http://www.mast.queensu.ca/∼murty/index2.html.
[6] P. Moree, *Artin's primitive root conjecture -a survey* - (2004) arXiv:math.NT, http://arxiv.org/abs/math/0412262, 30 pages.