2.12 Basic Sieve Theory

Last updated: 2020–11–02

How do we determine if an given element is irreducible? The ***sieve of Eratosthenes*** is a method of determining the primes less than a given number n. List the integers from 2 to n. The smallest entry 2 is prime. Cross out the multiplies of 2 from our list. The smallest remaining entry 3 is prime because it is not divisible by any smaller prime. Cross out the multiples of 3. Repeat.

The Greek polymath, Eratosthenes of Cyrene (276BCE–194BCE), is famous for his work on prime numbers and for measuring the diameter of the earth.

Using this method, Table 2.3 list the prime integers less than 100.

	$\boxed{2}$	$\boxed{3}$	~~4~~	$\boxed{5}$	~~6~~	$\boxed{7}$	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	

Table 2.3: The 25 primes less than 100

For any prime integer p, this method also allows one to identify the irreducible polynomials in $\mathbb{F}_p[x]$. List all polynomials by degree and then cross out products. Table 2.4 lists the irreducible polynomials of degree at most 4 in $\mathbb{F}_2[x]$.

~~0~~	~~1~~	x	$x+1$
~~x^2~~	~~x^2+1~~	~~x^2+x~~	x^2+x+1
~~x^3~~	~~x^3+1~~	~~x^3+x~~	x^3+x+1
~~x^3+x^2~~	x^3+x^2+1	~~x^3+x^2+x~~	~~x^3+x^2+x+1~~
~~x^4~~	~~x^4+1~~	~~x^4+x~~	x^4+x+1
~~x^4+x^2~~	~~x^4+x^2+1~~	~~x^4+x^2+x~~	~~x^4+x^2+x+1~~
~~x^4+x^3~~	x^4+x^3+1	~~x^4+x^3+x~~	~~x^4+x^3+x+1~~
~~$x^4+x^3+x^2$~~	~~$x^4+x^3+x^2+1$~~	~~$x^4+x^3+x^2+x$~~	$x^4+x^3+x^2+x+1$

Table 2.4: Irreducible polynomials in $\mathbb{F}_2[x]$ having small degree

2.12.1 Remark. Since x^2+x+1 is irreducible in $\mathbb{F}_2[x]$, the quotient $K := \mathbb{F}_2[x]/\langle x^2+x+1\rangle$ is a field. If α denotes the image of x in K, then $\{1, \alpha\}$ forms a basis of K over $\mathbb{F}_2$. Hence, the field K has four elements; namely $\{0, 1, \alpha, 1+\alpha\}$.

2.12.2 Theorem. *Let p be a prime integer. If N_d denotes the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ having degree d, then we have*

$$\sum_{d|n} d\, N_d = p^n .$$

Proof. Consider the formal power series $\sum_g t^{\deg(g)} \in \mathbb{Z}[[t]]$ where the summation is over all monic polynomials $g \in \mathbb{F}_p[x]$. The total

number of monic polynomials $g \in \mathbb{F}_p[x]$ of degree n is p^n, so we have

$$\sum_g t^{\deg(f)} = \sum_{n=0}^{\infty} p^n\, t^n = \frac{1}{1-p\,t}\,.$$

The polynomial ring $\mathbb{F}_p[x]$ is a unique factorization domain. As a consequence, we obtain

$$\sum_g t^{\deg(g)} = \prod_f (1-t^{\deg(f)})^{-1} = \prod_{d=1}^{\infty} (1-t^d)^{-N_d}$$

where the middle product runs over the monic irreducible polynomials in $f \in \mathbb{F}_p[x]$. It follows that

$$\frac{1}{1-p\,t} = \prod_{d=1}^{\infty} (1-t^d)^{-N_d}\,,$$

Taking logarithms gives

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{p^n\, t^n}{n} &= -\log(1-p\,t) = -\sum_{d=1}^{\infty} N_d\, \log(1-t^d) \\ &= \sum_{d=1}^{\infty}\sum_{e=1}^{\infty} d\, N_d\, \frac{t^{de}}{de} = \sum_{n=1}^{\infty} \frac{t^n}{n} \left(\sum_{de=n} d\, N_d \right). \qquad \square\end{aligned}$$

2.12.3 Definition. For any positive integer n, the ***Möbius function*** $\mu(n)$ is defined to be the sum of the primitive n-th roots of unity. It has values in $\{-1, 0, 1\}$ depending on the prime factorization of n:

- $\mu(n) = 1$ if n is a square-free positive integer with an even number of prime factors.
- $\mu(n) = -1$ if n is a square-free positive integer with an odd number of prime factors.
- $\mu(n) = 0$ if n has a squared prime factor.

The sum of the Möbius function over all positive divisors of n (including n itself and 1) is zero except when $n = 1$:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

2.12.4 Corollary. *Let p be a prime integer. If N_n denotes the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ having degree n, then we have*

$$N_n = \frac{1}{n} \sum_{d|n} \mu(d)\, p^{n/d}\,.$$

Proof. Combine Theorem 2.12.2 and Möbius inversion formula. $\square$

2.12.5 Theorem. *Let p be a prime integer and, for some positive integer d, set $q := p^d$. Every monic irreducible polynomial of degree d in $\mathbb{F}_p[x]$ is a factor of $x^q - x$. The irreducible factors of $x^q - x$ in $\mathbb{F}_p[x]$ are precisely the monic irreducible polynomials in $\mathbb{F}_p[x]$ whose degree divides d.*

Sketch of Proof. Since $(d/dx)(x^q - x) = qx^{q-1} - 1 = -1$, this monic polynomial has no multiple roots. Hence, its splitting field has q elements. $\square$

2.13 Irreducibility Criteria

Last updated: 2020–11–03

Can we identify and irreducible polynomial without enumerating all irreducible polynomial of lower degree?

2.13.1 Problem. Is $f(x) = x^3 + 6x^2 + 7 \in \mathbb{Z}[x]$ irreducible?

Solution. Yes. Otherwise f would have linear factor and its root would divide 7. However, we have $f(1) = 14$, $f(-1) = 12$, $f(7) > 0$, and $f(-7) = (-1)(49) + 7 < 0$. □

2.13.2 Proposition. *Let $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ and let p be a prime element in R that does not divide a_n. If the image of the polynomial f in $R/\langle p\rangle[x]$ is irreducible, then f is irreducible in $R[x]$.*

Proof. The canonical ring homomorphism $R \to R/\langle p\rangle$ induces a ring map $\varphi : R[x] \to R/\langle p\rangle[x]$. If we have $f = gh \in R$, then we obtain $\varphi(f) = \varphi(g)\,\varphi(h)$. The assumption that p does not divide a_n implies that $\deg \varphi(g) = \deg(g)$ and $\deg \varphi(h) = \deg(h)$. Hence, reducibility of the polynomial f leads to the reducibility of $\varphi(f)$. □

2.13.3 Problem. Is $x^4 + 15x^3 + 7 \in \mathbb{Q}[x]$ irreducible?

Solution. The image of this polynomial in $\mathbb{F}_5[x]$ is $x^4 + 2$. By evaluating $x^4 + 1$ at all five elements of $\mathbb{F}_5$, we see that $x^4 + 1$ has no root in $\mathbb{F}_5$. Suppose that $x^4 + 2 = (x^2 + a\,x + b)(x^2 + c\,x + d)$. It follows that $a + c = 0$, $ac + b + d = 0$, $ad + bc = 0$, and $bd = 2$. Since $c = -a$, we have $0 = ad + bc - a(d - b)$, so $a = 0$ or $d = b$.

- If $a = 0$, then we have $c = 0$. The equations $b + d = 0$ and $bd = 2$ imply that $d = -b$, $-b^2 = 2$, and $b^2 = 3$. However, $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$, and $4^2 = 1$. Hence, there is no element $b \in \mathbb{F}_5$ such that $b^2 = 3$.
- If $b = d$, then we have $b^2 = 2$. This is again impossible because the only perfect squares in $\mathbb{F}_5$ are 0, 1, and 4.

We see that the polynomial $x^4 + 2$ is irreducible in $\mathbb{F}_5[x]$. Thus, Proposition 2.13.2 shows that $x^4 + 15\,x^3 + 7$ is irreducible in $\mathbb{Z}[x]$ and Lemma 2.11.2 shows that it is irreducible in $\mathbb{Q}[x]$. □

2.13.4 Theorem (Schönemann–Eisenstein Criterion). *Let R a domain and let $f := a_0 + a_1\,x + \cdots + a_n\,x^n \in R[x]$ be a primitive polynomial of positive degree n. When there exists a prime ideal P in R such that*

- $a_n \notin P$,
- $a_0, a_1, \ldots, a_{n-1} \in P$, *and*
- $a_0 \notin P^2$,

the polynomial f is irreducible in $R[x]$.

Theodor Schönemann first published a version of this criterion in 1846. Gotthold Eisenstein published a somewhat different version in the same journal in 1850.

Proof. Suppose that $f = g\,h$ for some $g, h \in R[x]$ having positive degree. Set $g := b_0 + b_1\,x + \cdots + b_r\,x^r$ and $h := c_0 + c_1\,x + \cdots + c_s\,x^s$

where $\deg(g) = r$ and $\deg(h) = s$. It follows that $a_0 = b_0 c_0 \in P$. Since P is a prime ideal, we have $b_0 \in P$ or $c_0 \in P$. Having both b_0 and c_0 belong to P would imply that $a_0 \in P^2$ contradicting our hypotheses. Without loss of generality, we may assume that $b_0 \in P$ and $c_0 \notin P$. If every coefficient of g was in P, then every coefficient of f would also be in P again contradicting our hypothesis. Let b_i be the first coefficient of g such that $b_i \notin P$. Since

$$a_i = b_i c_0 + b_{i-1} c_1 + \cdots + b_0 c_i \,,$$

we obtain the equation $b_i c_0 = a_i - b_{i-1} c_1 - \cdots - b_0 c_i$. Every element on the right side of this equation lies in P. However, this implies that $b_i c_0 \in P$ which because P is prime yields either $b_i \in P$ or $c_0 \in P$ which is a contradiction. □

The following special case

2.13.5 Corollary. *Let R be a unique factorization domain with fraction field K and consider $f := a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. When there exists a prime $p \in R$ such that*
- *p does not divide a_n,*
- *p divides a_i for all $0 \leqslant i \leqslant n-1$, and*
- *p^2 does not divide a_0,*

then the polynomial f is irreducible in $K[x]$.

Proof. Theorem 2.13.4 shows that the polynomial f is irreducible in $R[x]$ and Lemma 2.11.2 shows that f is irreducible in $K[x]$. □

2.13.6 Problem. Is $x^5 - 6x^4 + 3 \in \mathbb{Q}[x]$ irreducible?

Solution. Yes, apply Corollary 2.13.5 with $p = 3$. □

2.13.7 Corollary. *For any prime integer p, the polynomial*

$$f := x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible in $\mathbb{Q}[x]$.

Proof. Since $(x-1) f(x) = x^p - 1$, the substitution $x \mapsto y + 1$ yields

$$y f(y+1) = (y+1)^p - 1 = y^p + \tbinom{p}{1} y^{p-1} + \tbinom{p}{2} y^{p-2} + \cdots + \tbinom{p}{p-1} y \,.$$

We have $\binom{p}{i} = p(p-1)\cdots(p-i+1)/i!$. If $i < p$, the the prime p is not a factor of $i!$, so $i!$ divides the product $(p-1)\cdots(p-i+1)$ which implies that $\binom{p}{i}$ is divisible by p. Dividing the expansion of $y f(y+1)$ by y shows that $f(y+1)$ statisfies the hypothesis of Corollary 2.13.5. Therefore, the polynomial $y^{p-1} + \binom{p}{1} y^{p-2} + \binom{p}{2} y^{p-3} + \cdots + \binom{p}{p-1}$ is irreducible and it follows that f also is. □