THE RING $\mathbb{Z}$ AND ITS QUOTIENTS

1. THE RING OF INTEGERS

The set $\mathbb{Z}$ with the two composition laws $+$ and $\times$ is a commutative ring. We have a euclidean division in $\mathbb{Z}$. For $a$ and $b$ in $\mathbb{Z}$, assuming $b \neq 0$, there exists a unique pair of integers $(q, r)$ such that $a = bq + r$ and $0 \leq r < b$. The integer $q$ is the quotient. And $r$ is the remainder.

Recall that an ideal of $\mathbb{Z}$ is a subset $I \subset \mathbb{Z}$ that is a subgroup for the $+$ law and such that for any $x \in \mathbb{Z}$ and $i \in I$ the product $xi$ belongs to $I$.

Using the euclidean division one proves that any ideal $I$ of $\mathbb{Z}$ is of the form $I = a\mathbb{Z} = \{ax | x \in \mathbb{Z}\}$ where $a$ is an integer called a generator of $I$. One says that $\mathbb{Z}$ is a principal ring. If $I$ is not the zero ideal $\{0\}$ then it has a unique positive generator. We call it the generator of $I$.

A unit in $\mathbb{Z}$ is an invertible element. Only 1 and $-1$ are units. A prime integer is a non-zero integer which is not a unit and has no positive divisor but 1 and itself. Any positive integer can be decomposed as a product of positive primes (with possible multiplicities) in a unique way, up to permutation of the factors. One says that $\mathbb{Z}$ is a factorial ring.

Call $\mathcal{P}$ the set of all positive primes.

If $M = \pm \prod_{p \in \mathcal{P}} p^{e_p}$ one says that $e_p$ is the $p$-valuation of $M$. On sometimes write $e_p = v_p(M)$. The 2-valuation of $12 = 2^2 \cdot 3$ is 2 and its 3 valuation is 1.

The greatest common divisor of $M = \prod_{p \in \mathcal{P}} p^{e_p}$ and $N = \prod_{p \in \mathcal{P}} p^{f_p}$ is

$$\text{gcd}(M, N) = \prod_{p \in \mathcal{P}} p^{\min(e_p, f_p)}.$$ 

The ideal generated by $M$ and $N$ is the smallest ideal containing $M$ and $N$. It is the set $\{\lambda M + \mu N | \lambda, \mu \in \mathbb{Z}\}$. It is equal to $\text{gcd}(M, N)\mathbb{Z}$. In particular there exists a pair of integers $(\lambda, \mu)$ such that $\lambda M + \mu N = \text{gcd}(M, N)$. The triple $(\text{gcd}(M, N), \lambda, \mu)$ can be computed from $M$ and $N$ using the extended euclidean algorithm.

The lowest common multiple of $M = \prod_{p \in \mathcal{P}} p^{e_p}$ and $N = \prod_{p \in \mathcal{P}} p^{f_p}$ is

$$\text{lcm}(M, N) = \prod_{p \in \mathcal{P}} p^{\max(e_p, f_p)}.$$ 

The intersection of $M\mathbb{Z}$ and $N\mathbb{Z}$ is an ideal of $\mathbb{Z}$. It is the ideal $\text{lcm}(M, N)\mathbb{Z}$.

It is evident that

$$\text{gcd}(M, N) \times \text{lcm}(M, N) = MN.$$
2. THE RING $\mathbb{Z}/N\mathbb{Z}$

Let $N \geq 2$ be an integer. The quotient of $\mathbb{Z}$ by $N\mathbb{Z}$ is a ring. The class $x + N\mathbb{Z}$ is often denoted $x \mod N$. The quotient ring $\mathbb{Z}/N\mathbb{Z}$ is finite. We denote $(\mathbb{Z}/N\mathbb{Z})^*$ the group of units (invertible elements) in $\mathbb{Z}/N\mathbb{Z}$. Recall $x \mod N$ is invertible if and only if $\gcd(x, N) = 1$. If this is the case we have two integers $\lambda$ and $\mu$ such that $\lambda x + \mu N = 1$ and $\lambda \mod N$ is the inverse of $x \mod N$ in $(\mathbb{Z}/N\mathbb{Z})^*$.

Computing the addition and subtraction of two classes $x \mod N$ and $y \mod N$ in $\mathbb{Z}/N\mathbb{Z}$ takes time $\leq K \log N$ for $K$ a constant.

Computing the multiplication of two classes $x \mod N$ and $y \mod N$ in $\mathbb{Z}/N\mathbb{Z}$ takes time $\leq K(\log N)^2$ for $K$ a constant using grade-school algorithm. Using fast arithmetic (based on Fourier transform) one can multiply in time $(\log N)^{1+o(1)}$.

The complexity of inverting modulo $N$ is $\leq K(\log N)^2$ for $K$ a constant using grade-school algorithms and $(\log N)^{1+o(1)}$ using advanced algorithms.

The complexity of computing $(a \mod N)^e$ is $\log e \times (\log N)^{1+o(1)}$ using fast arithmetic and fast exponentiation. Since $e$ is usually of the same order of magnitude as $N$ this complexity is essentially quadratic in $\log N$.

The group of units $(\mathbb{Z}/N\mathbb{Z})^*$ is cyclic when $N$ is a prime, because this group is a finite group of roots of unity in a field.

2.1. Chinese remainders. Assume $M \geq 2$ and $N \geq 2$ are coprime integers. We define a map $f : \mathbb{Z}/MN\mathbb{Z} \to (\mathbb{Z}/M\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ by $f(x \mod MN) = (x \mod M, x \mod N)$. It is easy to check that $f$ is well defined and injective. To prove that $f$ is surjective we consider the Bezout coefficients $\lambda$ and $\mu$ such that $\lambda M + \mu N = 1$ and we notice that $\lambda M$ is congruent to 0 modulo $M$ and to 1 modulo $N$. And $\mu N$ is congruent to 1 modulo $M$ and to 0 modulo $N$. Given any pair $c = (x \mod M, y \mod N)$ we check that $f(x \mu N + y \lambda M) = c$. So the map $f$ is surjective.

We have a ring isomorphism between $\mathbb{Z}/MN\mathbb{Z}$ and $(\mathbb{Z}/M\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$.

2.2. Euler’s function. For $N \geq 2$ we denote $\varphi(N)$ the order of the group $(\mathbb{Z}/N\mathbb{Z})^*$ of units in $\mathbb{Z}/N\mathbb{Z}$. A consequence of Chinese remainder theorem is that

$$\varphi(MN) = \varphi(M) \varphi(N)$$

when $\gcd(M, N) = 1$.

One checks that $\varphi(p^k) = p^{k-1}(p - 1)$ for every prime $p$ and integer $k \geq 1$.

Alltogether if $N = \prod_{p \in \mathbb{P}} p^{\nu_p}$ then $\varphi(N) = \prod_{p \in \mathbb{P}} p^{\nu_p - 1}(p - 1)$.

2.3. Lagrange’s theorem. Assume $G$ is a finite group and $H \subseteq G$ a subgroup. We define a relation $\mathcal{R}$ on $G$ by setting $x \mathcal{R} y$ for $x$ and $y$ in $G$ if and only if $y^{-1}x \in H$. This is an equivalence relation. The equivalent class of $x$ is $xH = \{xh | h \in H\}$. So every equivalence class has order $|H|$. And the equivalence classes form a partition of $G$. So the cardinality of $G$ is the product of $|H|$ times the number of classes.

We deduce that every subgroup of a finite group $G$ has order dividing $|G|$.

Consider now an element $g$ in $G$. The smallest subgroup of $G$ containing $g$ is denoted by $\langle g \rangle$. It is the set of all powers (positive or negative) of $g$. This is the set $\{1, g, g^2, \ldots, g^{o-1}\}$ where $o$ is the smallest positive integer such that $g^o = 1$.
Indeed the map $E : \mathbb{Z} \to G$ that sends $n$ onto $g^n$ is a group homomorphism. Its image is $\langle g \rangle$. Its kernel is a non trivial ideal of $\mathbb{Z}$. We denote by $o$ the positive generator of this kernel. This is called the order of $g$.

Because $\langle g \rangle$ is a subgroup of $G$ its order $o$ divides $|G|$. So $|G| = oq$ for some integer $q$ and $g^{(G)} = g^{oq} = (g^o)^q = 1$. We have proved the following theorem.

**Theorem 1** (Lagrange). *If $G$ is a finite group and $g$ an element in $G$ then $g^{(G)} = 1$.***

2.4. **Fermat’s and Euler’s theorems.** Assume $N \geq 2$ is a positive integer. The group of units $(\mathbb{Z}/N\mathbb{Z})^*$ has order $\varphi(N)$ so for every integer $x$ that is prime to $N$ the class $x \mod N$ is in $(\mathbb{Z}/N\mathbb{Z})^*$ and according to Lagrange’s theorem its power $\varphi(N)$ is 1.

**Theorem 2** (Euler). *Let $N \geq 2$ be an integer. Let $N = \prod_{p \in P} p^{e_p}$ be the prime decomposition of $N$ and set $\varphi(N) = \prod_{p \in P} p^{e_p}(p - 1)$. Let $x$ be a prime to $N$ integer. Then $x^{\varphi(N)} = 1 \mod N$.*

In case $N$ is prime we obtain Fermat’s theorem.

**Theorem 3** (Fermat). *Let $N \geq 2$ be a prime integer. Let $x$ be a prime to $N$ integer. Then $x^{N-1} = 1 \mod N$.*

We deduce from Fermat’s theorem a method to prove that an integer is not prime. If we exhibit some integer $x$ that is prime to $N$ and such that $x^{N-1} \not\equiv 1 \mod N$, then $N$ is composite. For example

```gp
> N = 2^8 + 1
%1 = 115792089237316195423570985008687907853269984665640564039457584007913129639937
> N = 3 * 11 * 17
%1 = 561
> for(k = 1, N - 1, if(gcd(N, k) == 1, print(Mod(k, N)^(N - 1))))
Mod(1, 561)
Mod(1, 561)
... Mod(1, 561)
```

It is important to notice that, using fast exponentiation, Fermat’s congruence can be checked in time $(\log N)^2 + o(1)$.

Notice also that it may happen that a composite number satisfies the Fermat property. Indeed

```gp
> N = 2^8 + 1
%1 = 115792089237316195423570985008687907853269984665640564039457584007913129639937
> for(k = 1, N - 1, if(gcd(N, k) == 1, print(Mod(k, N)^(N - 1))))
Mod(1, 561)
Mod(1, 561)
... Mod(1, 561)
```

So we must refine on Fermat’s theorem if we want to make it useful to distinguish prime integers from composite ones.
2.5. The Miller-Rabin test. Since Fermat’s theorem is not strong enough to distinguish primes from composite numbers one tries to refine on it.

Assume \( N \) is an odd prime integer. Set

\[ N - 1 = 2^k m \]

with \( k \geq 1 \) and \( m \) odd. Take some \( x \) in \((\mathbb{Z}/N\mathbb{Z})^*\). According to Fermat’s theorem

\[ x^{N-1} - 1 = 0. \]

So

\[ x^{m2^k} - 1 = (x^{m2^{k-1}} - 1)(x^{m2^{k-1}} + 1) = 0. \]

Since \( \mathbb{Z}/N\mathbb{Z} \) is a field, one has

\[ x^{m2^{k-1}} - 1 = 0 \text{ or } x^{m2^{k-1}} + 1 = 0. \]

In the first case, assuming \( k \geq 2 \) we can go on factoring

\[ x^{m2^{k-1}} - 1 = (x^{m2^{k-2}} - 1)(x^{m2^{k-2}} + 1) = 0, \]

so

\[ x^{m2^{k-2}} - 1 = 0 \text{ or } x^{m2^{k-2}} + 1 = 0, \]

and so on.

At the end we have proven that if \( N \) is an odd prime and \( x \) is prime to \( N \) then

\[ x^m = 1 \text{ or } x^{m2^i} = -1 \text{ for some } 0 \leq i \leq k - 1. \]

If this is the case we say that MR\((N, x)\) holds true. If there exists an integer \( x \) prime to \( N \) such that MR\((N, x)\) does not hold true then \( N \) is composite.

We call MR\((N, x)\) the Miller-Rabin condition for \( N \) and \( x \).

For example assume \( N = 29 \). Then \( k = 2 \) and \( m = 7 \). Choose \( x = 2 \), and check that \( 2^{14} = -1 \mod 29 \). So MR\((29, 2)\) is true.

Note that even if \( N \) is composite, there might exist some \( x \) such that MR\((N, x)\) is true. However, Monier has proved that if \( N \geq 15 \) is odd and composite then at most one fourth of the units in \( \mathbb{Z}/N\mathbb{Z} \) satisfy the Miller-Rabin condition MR\((N, x)\). These are called the false witnesses.

So in order to test whether and odd integer \( N \) is prime we pick random elements \( x \) in \((\mathbb{Z}/N\mathbb{Z})^*\) and check the Miller-Rabin condition MR\((N, x)\). Since three fourth of the units fail to satisfy this condition the probability of missing a composite is \( \leq 1/4 \).

After a few dozens such tests we can either prove that \( N \) is composite or convince ourselves that it is prime.

The condition MR\((N, x)\) can be tested at the expense of \((\log N)^{2+o(1)}\) elementary operations using fast arithmetic and fast exponentiation.

The class RP consists of all languages such that there exists a polynomial time Turing machine \( M \) that takes as input a word \( w \) and some auxiliary seed \( s \). When \( w \) is not in \( L \) the machine always rejects it whatever \( s \) could be. When \( w \) is in \( L \) the machine will accept if for at least one half of the values of \( s \). It may reject if for the remaining values of \( s \).

The class co–RP consists of all languages whose complementary language belongs to RP. It is easily checked that the intersection of RP and co–RP is ZPP.
The existence of Miller-Rabin condition proves that the language PRIME consisting of all prime integers is in $\text{co-RP}$.

Agrawal, Kayal and Saxena have proved that PRIME is in $\text{P}$.

3. DENSITY OF PRIME INTEGERS

Remind the size of a positive integer may be defined as the number of digits in its decimal representation, that is $\lceil \log_{10}(a + 1) \rceil$.

It is known since antiquity that there exist infinitely many prime integers. On may ask how many primes can be found in the interval $[1, A]$. We note $\pi(A)$ this number. Hadamard and de la Vallée-Poussin have proven that

$$\pi(A) = \frac{A}{\log A} (1 + o(1)).$$

This is confirmed by experiments.

<table>
<thead>
<tr>
<th>$A$</th>
<th>10</th>
<th>100</th>
<th>1000</th>
<th>10000</th>
<th>100000</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\pi(A)$</td>
<td>4</td>
<td>25</td>
<td>168</td>
<td>1229</td>
<td>9592</td>
</tr>
<tr>
<td>$A/\pi(A)$</td>
<td>2.5</td>
<td>4</td>
<td>5.95</td>
<td>8.14</td>
<td>10.4</td>
</tr>
<tr>
<td>$\log A$</td>
<td>2.3</td>
<td>4.6</td>
<td>6.9</td>
<td>9.2</td>
<td>11.5</td>
</tr>
</tbody>
</table>

So a random integer in the interval $[A, 2A]$ is prime with probability close to $1/\log(A)$.

A good way of finding a random prime of a given size is to pick random elements in $[A, 2A]$ and test them for the Miller-Rabin condition. Since the complexity of such a test is $(\log A)^{2+o(1)}$ and the probability of success is $(\log A)^{-1+o(1)}$ the total time of this search is $(\log A)^{3+o(1)}$ using fast arithmetic, and $(\log A)^{4+o(1)}$ using grade-school algorithms.

REFERENCES
