Introduction to Algebraic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

The Natural Numbers

Divisibility, Factors and Multiples

- We take the natural numbers to be $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Definition

Let a and b be integers. Then b **divides** a, or b is a **factor** or **divisor** of a, if

$$a = bc, \quad \text{for some integer } c.$$

Write $b \mid a$ to mean that b divides a and $b \nmid a$ to mean that b does not divide a. When b divides a, we also say that a is a **multiple** of b.

- If $b \mid a$, then $-b \mid a$.

  So the non-zero divisors of an integer occur naturally in pairs.
- Clearly, if $b \neq 0$, then $b \mid a$ means that the remainder when a is divided by b is 0.

Example

- We have $323 = 17 \times 19$.

  So $17 \mid 323$.

  On the other hand, $17 \nmid 324$.
- For all $a \in \mathbb{Z}$, we have:
  - $1 \mid a$ (since $a = 1 \cdot a$);
  - $a \mid a$ (since $a = a \cdot 1$);
  - $a \mid 0$ (since $0 = a \cdot 0$).

  Notice that $0 \nmid a$, if $a \neq 0$.

Prime Numbers

Definition

A **prime number** is a natural number $p > 1$ which is not divisible by any natural number other than 1 and p itself.
A **composite number** is a natural number $n \neq 1$ which is divisible by natural numbers other than 1 and itself.
1 is neither prime nor composite.

Example: 37 is prime

$39 = 3 \times 13$ is composite.

Euclid's Theorem

Theorem (Euclid)

There are infinitely many prime numbers.

- Suppose that there are only finitely many primes, $p_1, p_2, \ldots, p_n$.

  Define
  $$N = p_1 p_2 \cdots p_n + 1.$$

  Suppose that p is a prime factor of N.

  N is 1 more than a multiple of each p_i.

  So none of the primes $p_1, \ldots, p_n$ is a factor of N.

  Hence, p is not one of the primes $p_1, \ldots, p_n$.

  So we have found another prime.

  This contradicts our assumption that $p_1, \ldots, p_n$ are all the primes.

  So there must be infinitely many primes.

Subsection 2

Euclid's Algorithm

Introducing Highest Common Factors

- Suppose integers a and b are both multiples of another integer c,

$$c \mid a \quad \text{and} \quad c \mid b.$$

- Then c is a **common factor** of a and b.

  Example: 8 and 36 have common factors ± 1, ± 2 and ± 4.
- The **highest common factor** is the largest of the common factors.

  Example: The highest common factor of 8 and 36 is 4.
- Unless both a and b are zero, there will be a highest common factor of a and b.
- This is denoted by (a, b).

Highest Common Factor

Definition

The integer $h = (a,b)$ is a **highest common factor** (or **greatest common divisor**) of given integers a,b if:

1. $h \mid a$ and $h \mid b$ (so h is a common factor of a and b);
2. if $c \mid a$ and $c \mid b$, then $c \leq h$ (if c is a common factor of a and b, then c is at most h).

- Clearly $(a,b) = (b,a)$.
- Moreover, when b is non-zero,

$$(0,b) = (b,b) = |b|.$$

Relative Prime Integers

Definition

Let a and b be integers. Say that a and b are **coprime** (or **relatively prime**) if

$$(a, b) = 1,$$

i.e., a and b have no common factor except $(\pm)1$.

Example: The numbers 10 and 21 are coprime.

The Division Algorithm

- An integer a can always be divided by a positive integer b to give a unique quotient q and a unique remainder r in the range $0 \leq r < b$:

$$a = qb + r, \qquad 0 \leq r < b.$$

- The quotient and remainder are always assumed to be integers.

  Example: We have:
  - $78 = 8(9) + 6$;
  - $-78 = -9(9) + 3$.
- The simple process of finding a quotient and remainder is known as the **division algorithm**.

Division Algorithm and Greatest Common Divisors

Lemma

Suppose that $a = qb + r$. Then $(a,b) = (b,r)$.

- Suppose that d divides a and b.

  Since $r = a - qb$, we also have $d \mid r$.

  Thus, every common divisor of a and b also divides r.

  In particular, (a,b) divides r.

  Since it also divides b, (a,b) is a common factor of b and r.

  So $(a,b) \leq (b,r)$, as (b,r) is the highest common factor of b and r.

  Conversely, any common divisor of b and r also divides $a = qb + r$.

  In particular, (b,r) divides a.

  As in the first paragraph, we conclude that $(b,r) \leq (a,b)$.

  Combining these inequalities, we see that $(a,b) = (b,r)$.

Euclid's Algorithm

- Repeatedly applying the division algorithm gives Euclid's algorithm, which computes highest common factors very efficiently.
  Example: We find the highest common factor of 630 and 132.
  - By the division algorithm, $630 = 4 \times 132 + 102$.
  - By the lemma, $(630, 132) = (132, 102)$.
  - By the division algorithm, $132 = 1 \times 102 + 30$.
  - By the lemma, $(132, 102) = (102, 30)$.
  - By the division algorithm, $102 = 3 \times 30 + 12$.
  - By the lemma, $(102, 30) = (30, 12)$.
  - By the division algorithm, $30 = 2 \times 12 + 6$.
  - By the lemma, $(30, 12) = (12, 6)$.
  - Finally, the division algorithm gives $12 = 2 \times 6 + 0$.
  - By the lemma $(12, 6) = (6, 0)$.

  The highest common factor of 0 and b is just $|b|$. So $(6, 0) = 6$.
  We conclude that

$$(630, 132) = (132, 102) = (102, 30) = (30, 12) = (12, 6) = (6, 0) = 6.$$

Euclid's Algorithm (Cont'd)

- Usually, we write the equations in tabular form:

$$\begin{aligned} 630 &= 4 \times 132 + 102 \\ 132 &= 1 \times 102 + 30 \\ 102 &= 3 \times 30 + 12 \\ 30 &= 2 \times 12 + 6 \\ 12 &= 2 \times 6 + 0. \end{aligned}$$

The highest common factor is the last non-zero remainder.

Euclid's Algorithm (Cont'd)

- By running the algorithm backwards, we can write the highest common factor as the sum of a multiple of 630 and a multiple of 132:

$$\begin{aligned} 6 &= 30-2\times 12 \\ &= 30-2\times(102-3\times 30) \\ &= 7\times 30-2\times 102 \\ &= 7\times(132-1\times 102)-2\times 102 \\ &= 7\times 132-9\times 102 \\ &= 7\times 132-9\times(630-4\times 132) \\ &= 43\times 132-9\times 630. \end{aligned}$$

Thus the highest common factor of 630 and 132 has been written in the form $630s+132t$, for certain integers s and t.

Euclid's Algorithm and Greatest Common Divisor

Theorem

Let $a, b \in \mathbb{Z}$, with $b \neq 0$. Then there exist $s, t \in \mathbb{Z}$, such that

$$(a, b) = sa + tb.$$

- By virtually the same argument as in the preceding example.

Characterization of Coprimality

- Recall that integers a and b are said to be *coprime* or *relatively prime* if their highest common factor (a,b) is 1.

Corollary

Let $a,b\in\mathbb{Z}$. Then a and b are coprime if and only if there exist integers s and t, such that
$$sa+tb=1.$$

- Suppose a and b are coprime.

  We have $(a,b)=1$.

  So there exist integers s and t, such that $sa+tb=1$.

  Conversely, suppose there exist s and t, such that $sa+tb=1$.

  A common factor of a and b will divide $sa+tb$.

  So it will divide 1.

  This implies that a and b are coprime.

Dividing out the Greatest Common Divisor

- We can use this result to prove several elementary properties of the highest common factor.

Corollary

Let $a, b \in \mathbb{Z}$, not both zero. If $h = (a, b)$, then $\frac{a}{h}$ and $\frac{b}{h}$ are coprime.

- By Euclid's algorithm, there exist integers s and t, such that

$$sa + tb = (a, b) = h.$$

So we get

$$s\frac{a}{h} + t\frac{b}{h} = 1.$$

Thus, $\frac{a}{h}$ and $\frac{b}{h}$ are coprime.

Coprimes and Products I

Lemma

Suppose that $(a, bc) = 1$. Then $(a, b) = 1$ and $(a, c) = 1$.

- Suppose a and bc are coprime.

  Then, there are integers s and t, such that

  $$sa + tbc = 1.$$

  But then

  $$sa + (tc)b = 1.$$

  Put $m = tc$, so that there are integers s and m, with

  $$sa + mb = 1.$$

  It follows that a and b must be coprime.

  Similarly, a and c are coprime, using the bracketing $sa + (tb)c = 1$.

Coprimes and Products II

Lemma

Suppose that $(a,b)=1$ and $(a,c)=1$. Then $(a,bc)=1$.

- If $(a,b)=1$, then there are integers s and t so that $sa+tb=1$.
  If $(a,c)=1$, then there are integers p and q so that $pa+qc=1$.
  Rearrange these:
  $$tb=1-sa, \qquad qc=1-pa.$$
  Then multiply:
  $$(tq)bc=1-sa-pa+spa^2=1-(s+p-spa)a.$$
  Set $m=s+p-spa$ and $n=tq$.
  This gives $ma+nbc=1$.
  Hence a and bc are coprime.

Coprimes and Divisibility

- The last consequence of the characterization of coprimes is very important.

Lemma

Suppose that $a \mid bc$ and $(a,b)=1$. Then $a \mid c$.

- Suppose $(a,b)=1$.
  Then there exist integers s and t, such that

$$sa+tb=1.$$

Multiply this equation by c to get

$$sac+tbc=c.$$

Notice that a clearly divides sac.
The hypothesis that $a \mid bc$ implies that a divides the left-hand side.
Since it is equal to c, we get that $a \mid c$.

Subsection 3

The Fundamental Theorem of Arithmetic

Products Divisible by a Prime

Lemma

Suppose that $p \mid ab$, where $a, b \in \mathbb{Z}$, and p is prime. Then either $p \mid a$ or $p \mid b$.

- If $p \mid a$, we are done. If $p \nmid a$, we need to show that $p \mid b$.

  Suppose $p \nmid a$.

  Any common divisor of a and p must divide p.

  But the only divisors of p are 1 and p.

  Since $p \nmid a$, the only possible common divisor is 1.

  We conclude that $(a, p) = 1$.

  Now we can write $sa + tp = 1$, for some integers s and t.

  Multiply by b to get $sab + tpb = b$.

  As $p \mid ab$, it divides the left-hand side. So $p \mid b$.

Generalized Products Divisible by a Prime

Corollary

Suppose that $p \mid a_1 a_2 \cdots a_n$. Then $p \mid a_i$, for some $i = 1, \ldots, n$.

- By repeated application of the preceding lemma.

The Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every integer n greater than 1 can be expressed uniquely (apart from the order of factors) as a product of primes.

- Suppose there is an integer n with two different factorizations.

  Divide out any primes occurring in both factorizations.

  We, thus, get an equality of the form

  $$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

  where the factors p_i and q_j are all primes, not necessarily all distinct, but where no prime on the left also occurs on the right.

The Fundamental Theorem of Arithmetic (Cont'd)

- But p_1 divides the left-hand side and therefore the right-hand side. So

  $$p_1 \mid q_1 \cdots q_s.$$

  By the preceding corollary, p_1 must divide one of the q_j.

  Now the only divisors of the prime q_j are 1 and q_j itself.

  Therefore, p_1 must be identical with one of the q_j.

  This contradicts the hypothesis that no prime occurs on both sides of the equality.

Prime Factorization: Examples

- Each integer $n > 1$ can be written uniquely in the form

$$n = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k},$$

where:

  - $p_1, p_2, \ldots, p_k$ are primes, with $p_1 < p_2 < \cdots < p_k$;
  - $n_1, n_2, \ldots, n_k$ are natural numbers.

Example: We have

$$\begin{array}{rcl} 360 & = & 2^3 \cdot 3^2 \cdot 5; \\ 4725 & = & 3^3 \cdot 5^2 \cdot 7; \\ 714420 & = & 2^2 \cdot 3^6 \cdot 5 \cdot 7^2. \end{array}$$

Subsection 4

The Gaussian Integers

The Gaussian Integers

- Fermat asked which natural numbers could be written as the sum of two squares.
- Given a natural number n, we ask whether there are integers a and b so that $n = a^2 + b^2$.
- Factorize the right side as a product of the two complex numbers $a + ib$ and $a - ib$.
- We are working in
$$Z[i] = \{x + iy : x, y \in \mathbb{Z}\}.$$
- We ask how the number n factorizes in the larger set $\mathbb{Z}[i]$.
- Elements of the set $\mathbb{Z}[i]$ are known as **Gaussian integers**.
- We define the **norm** of $x + iy$
$$N(x+iy) = |x+iy|^2 = (x+iy)\overline{(x+iy)} = (x+iy)(x-iy) = x^2 + y^2.$$

Closure Under Product for Sum of Squares

Lemma

Suppose that n_1 and n_2 can be written as the sum of two squares. Then their product $n_1 n_2$ is also the sum of two squares.

- Suppose that $n_1 = a^2 + b^2$ and that $n_2 = c^2 + d^2$.

  Equivalently,

$$\begin{aligned} n_1 &= N(a+ib) = (a+ib)\overline{(a+ib)}; \\ n_2 &= N(c+id) = (c+id)\overline{(c+id)}. \end{aligned}$$

  Multiplication of complex numbers is commutative.

  So we get

$$|zw|^2 = zw\overline{zw} = z\overline{z}w\overline{w} = |z|^2|w|^2.$$

Closure Under Product for Sum of Squares (Cont'd)

- We showed that

$$N(zw) = N(z)N(w).$$

In particular, we have

$$N((a+ib)(c+id)) = N(a+ib)N(c+id) = n_1 n_2.$$

Moreover,

$$N((a+ib)(c+id)) = N((ac-bd)+i(ad+bc)) = (ac-bd)^2 + (ad+bc)^2.$$

Combining these gives

$$n_1 n_2 = (a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2.$$

Necessary Condition for Being Sum of Two Squares

- The lemma suggests that we should start by working out the prime numbers p which can be written as the sum of two squares.
- Clearly, $p = 3$ cannot be written as the sum of two squares.
- Square numbers give a remainder which is 0 or 1 modulo 4.
- So the only possible sums of two squares are

$$0+0, \quad 0+1, \quad 1+1 \mod 4.$$

- No number which is 3 (mod 4) can be written as a sum of two squares.
- We next show in order:
  - A Euclidean Algorithm for Gaussian Integers;
  - A divisibility property of products of Gaussian Integers;
  - Every prime $p \equiv 1 \pmod 4$ can be written as a sum of two squares.

Euclidean Algorithm for Gaussian Integers

Lemma

Let $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$. Then there exist Gaussian integers κ and ρ, such that

$$\alpha = \kappa\beta + \rho, \quad N(\rho) < N(\beta).$$

- We start by finding $\kappa \in \mathbb{Z}[i]$, with $|\frac{\alpha}{\beta} - \kappa| < 1$.

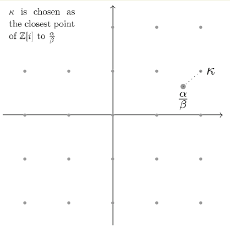
  Take the quotient $\frac{\alpha}{\beta} = x + iy \in \mathbb{C}$.

  Choose integers m and n, such that

  $$|x - m| \le \frac{1}{2}, \quad |y - n| \le \frac{1}{2}.$$

  Write $\kappa = m + in \in \mathbb{Z}[i]$ and $\rho = \alpha - \kappa\beta$.

  This makes κ the closest point of $\mathbb{Z}[i]$ to $\frac{\alpha}{\beta}$.



Euclidean Algorithm for Gaussian Integers (Cont'd)

- Now we have

$$\begin{aligned} \left|\frac{\alpha}{\beta} - \kappa\right| &= |(x+iy) - (m+in)| \\ &= |(x-m) + i(y-n)| \\ &\leq \sqrt{(\tfrac{1}{2})^2 + (\tfrac{1}{2})^2} \\ &= \frac{1}{\sqrt{2}}. \end{aligned}$$

So,

$$\begin{aligned} N(\rho) &= |\rho|^2 \\ &= |\alpha - \kappa\beta|^2 \\ &= \left|\frac{\alpha}{\beta} - \kappa\right|^2 |\beta|^2 \\ &\leq \frac{1}{2}|\beta|^2 \\ &< |\beta|^2 \\ &= N(\beta). \end{aligned}$$

Divisibility Property of Products in Gaussian Integers

Proposition

If $\pi \mid \alpha\beta$ in $\mathbb{Z}[i]$, for a prime π, then $\pi \mid \alpha$ or $\pi \mid \beta$.

- If $\pi \mid \alpha$, we are done. If $\pi \nmid \alpha$, we need to show that $\pi \mid \beta$.

  Suppose $\pi \nmid \alpha$.

  A common divisor of α and π must divide π.

  However, the only divisors of π are 1 and π.

  Since $\pi \nmid \alpha$, the only possible common divisor is 1.

  It follows that $(\alpha, \pi) = 1$.

  Write $\sigma\alpha + \tau\pi = 1$, for some Gaussian integers σ and τ.

  Multiply by β to get $\sigma\alpha\beta + \tau\pi\beta = \beta$.

  As $\pi \mid \alpha\beta$, it divides the left side which equals the right side.

  So $\pi \mid \beta$.

Primes $p \equiv 1 \pmod 4$ as Sums of Two Squares

Theorem

Every prime $p \equiv 1 \pmod 4$ can be written as the sum of two squares.

- Since $p \equiv 1 \pmod 4$, we can solve the equation

$$x^2 + 1 \equiv 0 \pmod p.$$

Write $p = 4k + 1$. Set $x = (2k)!$. Then,

$$\begin{aligned}
(2k)!(2k)! &= 1 \cdot 2 \cdots (2k-1)(2k)(2k)(2k-1) \cdots 2 \cdot 1 \\
&= (-1)^{2k} 1 \cdot 2 \cdots (2k-1)(2k)(2k)(2k-1) \cdots 2 \cdot 1 \\
&= (-1)(-2) \cdots (-2k+1)(-2k)(2k)(2k-1) \cdots 2 \cdot 1 \\
&\equiv (p-1)(p-2) \cdots (2k+2)(2k+1)(2k)(2k-1) \cdots 2 \cdot 1 \\
&\qquad \pmod p \\
&\equiv (p-1)! \pmod p \\
&\equiv -1 \pmod p. \quad \text{(Wilson's Theorem)}
\end{aligned}$$

Thus, $x^2 \equiv -1 \pmod p$ as required.

Primes $p \equiv 1 \pmod 4$ as Sums of Two Squares (Cont'd)

- With this value of x, $p \mid x^2 + 1 = (x+i)(x-i)$ in $\mathbb{Z}[i]$.

  Suppose p is prime in $\mathbb{Z}[i]$.

  Then we would have $p \mid x+i$ or $p \mid x-i$.

  But $\frac{x \pm i}{p} \notin \mathbb{Z}[i]$, as neither the real nor imaginary parts are integers.

  This gives a contradiction.

  So p is not prime, and it therefore factorizes in $\mathbb{Z}[i]$.

  Suppose that p factorizes as $\alpha\beta$.

  Then $N(p) = p^2 = N(\alpha)N(\beta)$.

  We have three possibilities:

  1. $N(\alpha) = 1, N(\beta) = p^2$;
  2. $N(\alpha) = p, N(\beta) = p$;
  3. $N(\alpha) = p^2, N(\beta) = 1$.

Primes $p \equiv 1 \pmod 4$ as Sums of Two Squares (Cont'd)

1. Suppose that $N(\alpha) = 1$, with $\alpha = a + ib$.
   The only solutions to $a^2 + b^2 = 1$ are $a = \pm 1,\ b = 0$ and $a = 0,\ b = \pm 1$.
   Thus, $\alpha = \pm 1$ or $\alpha = \pm i$.
   So $\beta = \pm p$ or $\pm ip$.
   This does not involve factorizing p.
   It only involves writing it in an equivalent way using units.
3. The case $N(\alpha) = p^2$ and $N(\beta) = 1$ is similar.
2. Thus, p must factorize as $\alpha\beta$ with $N(\alpha) = N(\beta) = p$.
   If we write $\alpha = a + ib$, we get
   $$p = N(\alpha) = a^2 + b^2.$$
   We have found a representation of p as the sum of two squares.

Integers Expresible as Sums of Two Squares

- The fact that every prime number $p \equiv 1 \pmod 4$ can be written as the sum of two squares is the key ingredient in the following classification of those integers which can be written as the sum of two squares.

Theorem

A natural number n can be written as the sum of two squares if and only if n has prime power factorization

$$n = \prod_p p^{n_p},$$

where n_p is even, for all primes $p \equiv 3 \pmod 4$.

Quadratic Residues and the Legendre Symbol

- A number a is a **quadratic residue modulo** p if the equation
$$x^2 \equiv a \pmod{p}$$
has two solutions.
- A number a is a **non-residue** if there are no solutions.
- The **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined by
$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{if } a \text{ is a quadratic residue,} \\ -1, & \text{if } a \text{ is not a quadratic residue.} \end{cases}$$
- Legendre symbols have various properties which enable them to be calculated easily.
- We list some in the following slide.

Properties of the Legendre Symbol

- Explicit Formula for $\left(\frac{-1}{p}\right)$:
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}.$$
- Explicit Formula for $\left(\frac{2}{p}\right)$:
$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}.$$
- Multiplicativity:
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$
- Quadratic Reciprocity: For p, q distinct odd primes,
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}.$$

Alternative Solution to $x^2 \equiv -1 \pmod{p}$

- We saw that $x = (\frac{p-1}{2})!$ gives a solution to $x^2 \equiv -1 \pmod{p}$.
- A better way uses Legendre symbols.
- Recall that, for all a not divisible by p,

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p}.$$

- By a result of Euler, we have:

$$a^{(p-1)/2} \equiv \begin{cases} +1, & \text{if } a \text{ is a quadratic residue,} \\ -1, & \text{if } a \text{ is not a quadratic residue.} \end{cases}$$

- That is, $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Alternative Solution to $x^2 \equiv -1 \pmod{p}$ (Cont'd)

- Compute the Legendre symbols $\left(\frac{a}{p}\right)$ for $a = 2$, $a = 3$, and so on, until you find one with
$$\left(\frac{a}{p}\right) = -1.$$
- Using the multiplicativity of the Legendre symbol, we can see that the smallest such a will be prime.
- Then
$$a^{(p-1)/2} \equiv -1 \pmod{p}.$$
- Recalling that $p \equiv 1 \pmod{4}$, we set
$$x = a^{(p-1)/4} \pmod{p}.$$
- Then $x^2 \equiv -1 \pmod{p}$.

Example

- Consider $p = 73$.

  We compute
  - $\left(\frac{2}{73}\right) = (-1)^{\frac{1}{8}(73^2-1)} = (-1)^{666} = 1$;
  - $\left(\frac{3}{73}\right) = (-1)^{\frac{1}{4}(3-1)(73-1)}\left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = 1$;
  - $\left(\frac{5}{73}\right) = (-1)^{\frac{1}{4}4\cdot 72}\left(\frac{73}{5}\right) = \left(\frac{3}{5}\right) = (-1)^{\frac{1}{4}2\cdot 4}\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{1}{8}8} = -1$.

  Now we set $x = 5^{18} \pmod{73}$.

  We compute this by successively squaring modulo 73:

$$5^2 \equiv 25, \quad 5^4 \equiv 25^2 \equiv 41, \quad 5^8 \equiv 41^2 \equiv 2, \quad 5^{16} \equiv 2^2 \equiv 4.$$

  Then

$$5^{18} = 5^{16} \cdot 5^2 \equiv 4 \cdot 25 \equiv 27 \pmod{73}.$$

  So $x = 27$ gives a solution to $x^2 \equiv -1 \pmod{73}$.

Subsection 5

Another Application of the Gaussian Integers

A Diophantine Equation

- Equations where only integer solutions are sought are known as **Diophantine equations**.
- We apply uniqueness of factorization in $\mathbb{Z}[i]$ to find all integer solutions to
$$x^3 = y^2 + 1.$$
Remark: This is a special case of **Catalan's conjecture**, which predicts that the only consecutive perfect powers are $8 = 2^3$ and $9 = 3^2$, proven by Preda Mihăilescu in 2002.

Factorization in $\mathbb{Z}[i]$

- Some care has to be taken in defining uniqueness of factorization.
- In $\mathbb{Z}[i]$, given a factorization
$$\alpha = \beta\gamma,$$
and u and v in $\mathbb{Z}[i]$ satisfying $uv = 1$, then we will consider
$$\alpha = (u\beta)(v\gamma)$$
as an equivalent factorization.
- In $\mathbb{Z}[i]$, the possible values of such units u are ± 1 or $\pm i$, exactly those elements u with $N(u) = 1$.

A Diophantine Equation: Some Observations

- Suppose that x and y are integers satisfying $x^3 = y^2 + 1$.

  Suppose x is even.

  Then $y^2 + 1 \equiv 0 \pmod 4$, which is not possible.

  So x is odd. Therefore, y is even.

  We make use of the theory of the Gaussian integers and use the word "prime" rather loosely, assuming that primes in $\mathbb{Z}[i]$ satisfy the same properties as prime numbers in $\mathbb{Z}$ do.

  In $\mathbb{Z}[i]$, we can write

  $$x^3 = (y+i)(y-i).$$

  We show that any common factor of $y+i$ and $y-i$ must be a unit ± 1 or $\pm i$ (i.e., $y+i$ and $y-i$ are coprime).

A Diophantine Equation: $y+i$ and $y-i$ are Coprime

- Recall $x^3 = y^2 + 1 = (y+i)(y-i)$, x odd and y even.

Lemma

Suppose that $\alpha \mid y+i$ and also $\alpha \mid y-i$. Then α is a unit.

- Suppose $\alpha \mid y+i$, $\alpha \mid y-i$, and that α is not a unit.
  Then $\alpha \mid ((y+i)-(y-i))$. So α is a factor of $2i = (1+i)^2$.
  Let $1+i = \beta\gamma$ be a factorization of $1+i$.
  It must satisfy $N(\beta)N(\gamma) = N(1+i) = 2$.
  So either $N(\beta) = 1$ or $N(\gamma) = 1$. Then β or γ is ± 1 or $\pm i$, a unit.
  So $1+i$ is a prime in $\mathbb{Z}[i]$.
  Now $\alpha \mid (1+i)^2$. Suppose α is not a unit.
  Then, by unique factorization in $\mathbb{Z}[i]$, $1+i \mid \alpha$.
  Hence, $1+i \mid x^3$. So $1+i \mid x$. But then $(1+i)^2 \mid x^2$. So $2i \mid x^2$.
  Thus, x^2 is even. This contradicts the observation that x is odd.

A Diophantine Equation: Determining the Solutions

- We now know that $y+i$ and $y-i$ are coprime (in the sense that any common divisor must be a unit).
  Suppose $\pi \mid x$ and π is a prime (so not a unit).
  Then $\pi^3 \mid x^3 = (y+i)(y-i)$.
  Now $y+i$ and $y-i$ have no factor in common.
  So either $\pi^3 \mid y+i$ and $\pi \nmid y-i$, or vice versa.
  In particular,
  $$y+i = u\beta^3, \qquad y-i = v\gamma^3,$$
  where u and v are units.
  Now the units ± 1 and $\pm i$ are all already cubes.
  So we can absorb them into β and γ.
  Therefore, we may assume that, for some integers a and b,
  $$y+i = (a+bi)^3.$$

Determining the Solutions (Cont'd)

- We found $y+i=(a+bi)^3$.
  Expanding, we get
  $$y+i=(a^3-3ab^2)+i(3a^2b-b^3).$$
  Equating imaginary parts gives
  $$(3a^2-b^2)b=1.$$
  The only way that a product of two integers can give 1 is if both are 1, or both are -1.
  - If $b=1$, there is no possible solution for a (we would need $3a^2=2$).
  - If $b=-1$, we see that $a=0$ gives the only solution.

  It follows that $y+i=(-i)^3=i$.
  So the only solution in integers to the original equation
  $$x^3=y^2+1$$
  is when $y=0$, which implies that $x=1$.