MATH 145 Notes

Alfred Menezes - Info
tinyurl.com/math145, Userid : math145, Passowrd : cat
MC 5029
M 3 - 4:30
T 2 - 3:30

1. Number Systems

Natural Numbers - Set of positive whole numbers. Closed under addition and multiplications, not closed under subtraction and ordinary division. Denoted $\mathbb{N}$

Prime Numbers - Numbers larger than 1 with no divisors other than 1 and itself.

Proposition 1. *(Euclid) There are infinitely many primes*

Proposition 2. *(Euclid)* Fundamental Theorem of Arithmetic *: Every natural number $n \geq 2$ has a unique prime factorization*

How to find a prime factorization efficiently? How do we efficiently confirm a prime factorization? How do we efficiently find large prime numbers? These and many questions will be investigates in class, and some are still open problems in mathematics.

Integers - Set of all whole numbers. Closed under addition, multiplication, and subtraction, but not division. Denoted $\mathbb{Z}$

Rational numbers - Denoted by $\mathbb{Q}$, it is the set $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$. Closed under all four standard operations.

We will see how to solve several equations. An example is $35x - 42y = 49$, which, when solved for integer solutions, requires the use of Euclid's Algorithm. Another example is finding all integer solutions to $y^2 + 2 = x^3$. A trivial solution to this is $(3,\ 5)$, but to prove it is the only integer solution we work in a quadratic number field (a field of the form $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Numbers like π are transcendental, or not the solution of any polynomial equation of rational coefficients. The real numbers include these numbers, and can be formally (but non-ideally) defined as the set of all infinite decimal expansions. We can also expand by adding i, which is the imaginary number with the property that $i^2 = 1$. The set of complex numbers (denoted $\mathbb{C}$) is defined by $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. The complex numbers cannot be extended again by adding a number that solves an unsolvable polynomial, as the next theorem states.

Proposition 3. Fundamental Theorem of Algebra*: Every polynomial equation with complex coefficients has a root in $\mathbb{C}$.*

2. Proof Techniques

Mathematical Induction

Axiom. (Well Ordering Theorem)
Every non-empty subset of $\mathbb{N}$ has a least element.

Proposition 4. (Principle of Mathematical Induction)
Let $P(n)$ be a statement that depends on $n \in \mathbb{N}$. Suppose 1) $P(1)$ is true, and 2) for each $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true. Then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof. See proof in MATH 147 notes

□

3. Integers and their properties

Terminology

Definition. *A* Commutative Ring $(R, +, \times)$ *consists of a set R and 2 binary operations $+ : R \times R \to R$ (addition) and $\times : R \times R \to R$ (multiplication) such that*

1. *Addition is commutative, $a + b = b + a$, $\forall a,\ b \in R$*
2. *Addition is associative $(a + b) + c = a + (b + c)$, $\forall a,\ b,\ c \in R$*
3. *There is a zero element (additive identity), $\exists 0 \in R : \forall a \in R(a + 0 = a)$*
4. *Each element has a negative (additive inverse), $\forall a \in R, \exists(-a) \in R : (a + (-a) = 0)$*
5. *Multiplication is commutative*
6. *Multiplication is associative*
7. *There is a unity element, $\exists 1 \in R : \forall a \in R(a \times 1 = a)$*

For example, the natural numbers under the standard operations is not a commutative ring. The integers, rational, reals, and complexes are all commutative rings, as well as the quadratic number field $\mathbb{Q}(\sqrt{2})$.

Definition. *A* field *is a commutative ring with two extra conditions*

1. *The zero and unity elements cannot be equal, $1 \neq 0$*
2. *There is a multiplicative inverse for each element, $\forall a \in R(\exists b \in R : a \times b = 1)$*

Now, the rationals, reals, complexes, and $\mathbb{Q}(\sqrt{2})$ are still fields, but $\mathbb{Z}$ is not a field. All of those mentioned sets happen to be infinite fields, we will see some finite fields later on. The advantage of this abstraction is that proving a theorem for one field proves properties for all fields, making it a very powerful tool.

The Integers

Definition. *Let $a,\ b \in \mathbb{Z}$. We say that a divides b if $\exists q \in \mathbb{Z}$ such that $b = qa$. This is written $a|b$. If no such q exists, we say a does not divide b, and we write $a \nmid b$.*

We have some interesting examples of this relation: for all $a \in \mathbb{Z}$, $1|a$, $a|0$, $0 \nmid a$ unless $a = 0$. The following are useful properties of divisibility.

Proposition 5. (Properties of divisibility)
Let $a,\ b,\ c \in \mathbb{Z}$, then:

1. *If $a|b$ and $b|c$, then $a|c$*
2. *If $a|b$ and $a|c$, then $a|(bx + cy)$, where $x,\ y \in \mathbb{Z}$. We call $bx + cy$ an integer linear combination of b and c*
3. *If $a|b$ and $b|a$, then $a = b$*
4. *If $a|b$ and $b \neq 0$, then $|a| \leq |b|$*

Proposition 6. (Division Algorithm)
Let $a \in \mathbb{N}$, $b \in \mathbb{Z}$. Then $\exists$ unique q, $r \in \mathbb{Z}$ such that $b = qa + r$, where $0 \leq r < a$

Proof. (Existence) Define $S = \{s | s = b - qa \geq 0,\ q \in \mathbb{Z}\}$. S is not empty because if $b \geq 0$ then $b - 0a \geq 0$, so $b \in S$. Also, if $b < 0$ then $s = b - ba = b(1 - a) \geq 0$, so $b - ba \in S$. By the well-ordering principle, there is a least element in S, which we denote $r = b - qa$. The number r is non-negative, since S only contatins non-negative numbers. Suppose $r \geq a$, then $b - (q + 1)a = b - qa - a = r - a \geq 0$ would be a smaller element of S, contradicting the minimality of r. Hence, we have that $0 \leq r < a$ and $b = qa + r$, as required.

(Uniqueness) Suppose we have q_1, q_2, r_1, r_2 with $b = q_1 + r_1$ and $b = q_2 + r_2$, $0 \leq r_1$, $r_2 < a$. Subtracting gives $(q_1 - q_2)a = r_2 - r_1$. Since both r_2 and r_1 are non-negative integers smaller than a, their difference must have $-a < r_2 - r_1 < a$. But the equation we obtained tells us that $r_2 - r_1$ is a multiple of a, and the only multiple of a is 0. Hence, $r_2 - r_1 = 0 \implies r_2 = r_1$, which in turn implies that $q_1 = q_2$ by substituting into the equation we obtained.

□

Note: If $a < 0$, we can write $b = q(-a) + r$, where $0 \leq r < -a$. This can also be rephrased as $b = (-q)a + r$ where $0 \leq r < -a$. Hence, a general form of the Division Algorithm tells us that we always have $b = qa + r$ where $0 \leq r < |a|$.

Definition. (Greatest Common Divisor)
The Greatest Common Divisor (GCD) of a and b, written $\gcd(a, b)$, is the largest integer that divides both a and b. We define $\gcd(0, 0) = 0$, to avoid problems with this special case.

For example, $\gcd(20, 30) = 10$, $\gcd(-20, 30) = 10$ (in general, $\gcd(a, b) = \gcd(|a|, |b|)$), $\gcd(0, b) = |b|$. If $a|b$, $\gcd(a, b) = |a|$. We also know that $\gcd(a, b) \geq 0$, and that $\gcd(a, b)$ always exists and is unique. Surprisingly, we have a simple, efficient algorithm for computing the GCD of any two integers, and it's 2300 years old.

Proposition 7. (Euclid's Algorithm)
Let a, b, q, $r \in \mathbb{Z}$ with $b = qa + r$. Then $\gcd(a, b) = \gcd(a, r)$

Proof. If $a = b = 0$, then the result is trivial. Otherwise, $d = \gcd(a, b)$. Since $d|a$ and $d|b$, then $d|(b - qa)$, so $d|r$. Hence, d is a common divisor of a and r. Let $c \in \mathbb{Z}$ such that $c|a$ and $c|r$. We see that $c|(qa + r)$, so $c|b$. Since c also divides a, it is a common divisor of a and b, so it must be that $c \leq d$. Hence, $\gcd(a, r) = d$

□

Euclid's algorithm takes the preceding theorem and iterates it until one of the two inputs to the GCD is 0, which gives an efficient and simple method to calculate the GCD of large numbers. The algorithm is guaranteed to terminate because the remainders that are obtained at each subsequent step form a strictly decreasing sequence.

Example: $1547 = 2 \cdot 560 + 427 \to 560 = 1 \cdot 427 + 133 \to 427 = 3 \cdot 133 + 28 \to 133 = 4 \cdot 28 + 21 \to 28 = 1 \cdot 21 + 7 \to 21 = 3 \cdot 7 + 0$, so the GCD of 1547 and 560 is 7.

The following show alternate definitions of the GCD:

Example: Find x and y such that $1547x + 560y = \gcd(1547, 560)$

We use the Extended Euclidean Alogrithm (EEA):

$\underline{x}$	$\underline{y}$	$\underline{r}$
1	0	1547
0	1	560
1	−2	427
−1	3	133
4	−11	28
−17	47	21
21	−58	7
−	−	0

Proposition 8. (Bezout's Identity)
Let a, $b \in \mathbb{Z}$. Then $\exists x$, $y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.

This last identity is proven by using the EEA.

Proposition 9. (GCD Characterization Theorem)
Let a, $b \in \mathbb{Z}$. Then $d = \gcd(a, b)$ if and onlt if 1) $d \geq 0$ 2) $d|a$ and $d|b$ 3) $\exists x$, $y \in \mathbb{Z}$ such that $d = ax + by$

Proof. If $\gcd(a, b) = d$, then 1) and 2) clearly hold, and 3) holds by Bezout's identity. In the other direction, we know that d is a common divisor of a and b. Consider any $c \in \mathbb{Z}$ such that $c|a$ and $c|b$, then $c|(ax + by) \implies c|d$. Now, if $d = 0$, then $a = b = 0$, so we have that $d = \gcd(a, b)$, and if $d \neq 0$ then since $c|d$ we have that $c \leq d$, and since this is true for any c, then $d = \gcd(1, b)$

□

Proof. Let a, $b \in \mathbb{Z}$. Then $d = \gcd(a, b)$ if and only if 1) $d \geq 0$, 2) $d|a$ and $d|b$, and 3) $(c|a) \wedge (c|b) \implies c|d$.

□

Linear Diophantine Equations

Problem: Given a, b, $c \in \mathbb{Z}$, find all integer solutions to $ax + by = c$

Proposition 10. *There exists a solution if and only if* $\gcd(a, b)|c$

Proof. (Linear Diphantine Equations 1)
Let $d = \gcd(a, b)$. Suppose (x_0, y_0) is an integer solution, so $ax_0 + by_0 = c$. Since $d|a$ and $d|b$, then $d|(ax_0 + by_0) \implies d|c$. On the other hand, if $d|c$, by Bezout's identity there are (x_0, y_0) integers such that $ax_0 + by_0 = d$. Let $c = dm$ with $m \in \mathbb{Z}$, then we have $a(mx_0) + b(my_0) = md = c$, so $(mx_0, my_0$ is an integer solution.

□

Proposition 11. (Linear Diphantine Equations 2)
Let a, b, $c \in \mathbb{Z}$, and let $d = \gcd(a, b)$, with $d|c$. We assume a and b are non-zero, and so d is non-zero, since that case is trivial. Then let (x_0, y_0) be one integer solution to

$ax + by = c$, as guaranteed to exist by the previous theorem. Then the set of all integer solutions is $\{(x, y) \mid x = x_0 + \frac{kb}{d},\ y = y_0 - \frac{ka}{d},\ k \in \mathbb{Z}\}$.

Lemma. *Let a, b, $c \in \mathbb{Z}$, and suppose $a|bc$ and $\gcd(a, b) = 1$. Then $a|c$.*

Proof. (of lemma)
Since $a|bc$, we can write $bc = az$ for some $z \in \mathbb{Z}$. Since $\gcd(a, b) = 1$, we can write $1 = ax + by$, with x, $y \in \mathbb{Z}$. Then $c = cax + cby = cax + azy = a(cx + zy)$, so $a|c$.

□

Lemma. *Let a, $b \in \mathbb{Z}$, not both 0, and let $d = \gcd(a, b)$. Then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.*

Proof. (of lemma)
We can write $d = ax + by$ where x, $y \in \mathbb{Z}$, by Bezout's identity. Dividing by d yields $1 = \frac{a}{d}x + \frac{b}{d}y$, and by the GCDCT, $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

□

Proof. (of theorem)
We can easily check that $(x_0 + \frac{kb}{d},\ y_0 - \frac{ka}{d})$ is a solution to $ax + by = c$. Now, let (x, y) be an arbitrary integer solution to $ax + by = c$. Let $X = x - x_0$ and $Y = y - y_0$. Now, $aX + bY = a(x - x_0) + b(y - y_0) = c - c = 0$, hence $aX = -bY$, and dividing by d yields $\frac{a}{d}X = -\frac{b}{d}Y$. Since $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, we have $\frac{a}{d}|Y$ and $\frac{b}{d}|X$. WLOG, assume $a \neq 0$ (otherwise do the following in opposite direction). The division implies we have $Y = \frac{a}{d}k$, for some $k \in \mathbb{Z}$, and substituting into $\frac{a}{d}X = -\frac{b}{d}Y$ yields $X = -\frac{b}{d}k$. These two can be rearranged into the forms $x = x_0 + \frac{kb}{d}$ and $y = y_0 - \frac{ka}{d}$).

□

In summary, we can use the Euclidean algorithm to find the existence of a solution to a linear Diophantine equation. We can also use the EEA to both find the existence of a solution and one particular example, which we can then combine with the result above to obtain the complete solution set of the linear Diophantine equation. Since the Euclidean algorithm is considered to be efficient (as will be proven later), this algorithm for solving linear Diophantine equations is considered efficient.

Prime Numbers

Definition. *An integer $p \geq 2$ is prime if its only positive divisors are 1 and p, otherwise p is composite.*

Proposition 12. *Let a, $b \in \mathbb{Z}$, and p be prime. If $p|ab$, then $p|a$ and/or $p|b$*

Proof. WLOG, suppose $p \nmid a$. Then $\gcd(a, b) = 1$. Then by a previous lemma, we have $p|b$, hence we have the desired result

□

Corollary. *Let a_1, a_2, $\cdots$, $a_n \in \mathbb{Z}$, and p be prime. If $p|a_1a_2a_3 \cdots a_n$, then $p|a_j$ for some $1 \leq j \leq n$*

Proposition 13. (Fundamental Theorem of Arithmetic)
Every integer $n \geq 2$ can be written as a product of primes, called a prime factorization. Moreover, n has a unique factorization, up to the order of the prime factors.

Proof. Suppose that not every $n \geq 2$ has a prime factorization. By the well-ordering theorem, we know that there is a smallest such number, which we call N. If N were prime, then its prime factorization would be N, so it must be composite, so we can write $N = ab$ for some $a, b \in \mathbb{Z}$ where $1 < a, b < N$. Since these numbers are smaller than N, the smallest integer with no prime factorization, they each must have a prime factorization. However, multiplying these prime factorizations gives us a series of prime factors that multiply to N, so we found a prime factorization of N, a contradiction. Hence, there exists a prime factorization for every $n \geq 2$.

Now we show the factorization's uniqueness. Clearly, 2 has a unique prime factorization. Suppose that the integers 2 ,3, 4, $\cdots$, k, where $k \geq 2$, have unique prime factorizations. Suppose $k+1$ has two prime factorizations, say $k+1 = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$. By a proposition above, since we have that $p_1 | q_1 q_2 \cdots q_s$, so $p_1 | q_j$ for some $1 \leq j \leq s$. WLOG, assume $p_1 | q_1$. Since these are both primes, it must then be that $p_1 = q_1$, so we can cancel them out from the original equation, yielding $\frac{k+1}{p_1} = p_2 p_3 \cdots p_r = q_2 q_3 \cdots qs$. This is a number smaller than $k+1$, which we know must have unique factorizations, so by the induction hypothesis we must have $r = s$ and $p_i = q_i$ for all $1 \leq i \leq r$. Hence $k+1$ also has a unique factorization.

□

As an example of an application, let $n \in \mathbb{N}$ and write $n = \prod_{i=1}^{k} p_i^{e_i}$, where p_i are pairwise distinct primes, and $e_i \geq 1$. Then the set of all positive divisors of n is $S = \{\prod_{i=1}^{k} p_i^{d_i} \mid 0 \leq d_i \leq e_i\}$. The proof will be required in Assignment #3. An interesting result from this is that the number of positive divisors is $(e_1+1)(e_2+1)\cdots(e_k+1)$.

Also, given two numbers represented as $a = \prod_{i=1}^{k} p_i^{a_i}$ and $b = \prod_{i=1}^{k} p_i^{b_i}$, where we allow the exponenets to be zero so we can have the same list of primes. Then the GCD of a and b is $d = \gcd(a,b) = \prod_{i=1}^{k} p_i^{d_i}$, where $d_1 = \min(a_1, b_1)$. This number is clearly larger than one and it divides a and b. Now, given any positive common divisor of a and b, which we call c, we have $c = \prod_{i=1}^{k} p_i^{c_i}$, where $c_i \leq a_i$ and $c_i \leq b_i$. Hence, $c_i \leq \min(a_1, b_1) = d_i$, and so c is a divisor of d. This proves that $d = \prod_{i=1}^{k} p_i^{d_i}$ is the GCD of a and b.

Proposition 14. *Let n, $k \in \mathbb{N}$. Then $\sqrt[k]{n}$ is either an integer or an irrational number.*

Proof. Suppose $\sqrt[k]{n} = \frac{a}{b}$, where a, $b \in \mathbb{N}$, $b \neq 0$, and $\gcd(a,b) = 1$. If $b = 1$, then $\sqrt[k]{n} = a \in \mathbb{N}$. Otherwise, then $b^k n = a^k$. Let p be a prime factor of b, then $p | a^n$ so by a lemma above, $p | a$. However, this would imply $p | \gcd(a,b)$, but $\gcd(a,b) = 1$, so we get a contradiction. Therefore, b must be equal to one if it is an integer, or otherwise the root is an irrational number.

□

Proposition 15. (Euclid's Theorem)
There are infintely many primes.

Proof. Suppose there are finitely many primes, calling them p_1, p_2, ..., p_k. Consider $N = p_1 p_2 \cdots p_k + 1$. Now, if p_i divides N, for some $1 \leq i \leq k$, then since $p_i | p_1 p_2 \cdots p_k$ we would have that $p_i | 1$, which is impossible. But, since N is larger than or equal to 2 (since it at least must contain the prime 2), it must have a prime factorization. Hence, N must be divisible by a prime that is not on the list, contradicting the completeness of the list of primes. Thus, there are infinitely many primes.

□

The largest known prime number is $2^{43112609} - 1$

We look at the following two statements:

Statement. *The prime numbers are irregularly distributed.*

Evidence 1) There are arbitrarily large gaps between successive primes. For instance, take $n \geq 3$. Consider the sequence of numbers $n! + 2$, $n! + 3$, ..., $n! + n$. These are all clearly composite numbers, thus giving us a gap of at least $n - 1$ between successive prime numbers.

Evidence 2) The Twin Prime Conjecture suggests that there are infinitely many primes p for which $p + 2$ is also a prime

Statement. *The prime numbers are regularly distributed*

Evidence 3) (Dirichlet's Theorem, 1837) Let a, $b \in \mathbb{N}$, with $\gcd(a, b) = 1$. Then there are infintely many primes of the form $an + b$, for $n \geq 0$. This is hard to prove for the general case, but it is relatively easy for some cases, such as $a = 2 \wedge b = 1$, $a = 3 \wedge b = 2$. The case $a = 4 \wedge b = 3$ can be proven using a modification of Euclid's theorem (see next assignment), as well as the case $a = 4 \wedge b = 1$ (see future assignment, maybe 4/5). For the general case, see PMATH 440, Analytic Number Theory.

Evidence 4) (Green-Tao, 2004) For each $k \in \mathbb{N}$, there is an arithmetic progression of primes having length k. In other words, $\exists$ primes b, $a + b$, $2a + b$, ..., $(k - 1)a + b$. For example, $(3, 5, 7)$ is of length 3, and $(5, 11, 17, 23, 29)$ is of length 5. The largest arithmetic progression known is $43142746595714191 + 5283234035979900n$, for $0 \leq n \leq 25$. The proof of this theorem guarantees that for any k there exists a k-term arithmetic progression of primes with largest prime at most $2^{2^{2^{2^{2^{100k}}}}}$. The Riemann hypothesis can remove one 2 from the iterated exponentiation

Evidence 5) (Prime number theorem) Let $\pi(x)$ be the number of primes in $[2, x]$. Then we have that $\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log(x)}} = 1$. So, $\pi(x) \approx \frac{x}{\log(x)}$

As an example, we prove a result weaker than the prime number theorem.

Proposition 16. *For $x \geq 2$, $\pi(x) > \log(\log(x))$*

Proof. Let p_n be the n-th prime number. We will prove by induction that $p_n \leq 2^{2^{n-1}}$, for $n \geq 1$. The proposition is clearly true for $n = 1$, by calculation. Suppose that $p_k \leq 2^{2^{n-1}}$ for all $k \leq n$, with $n \geq 1$. Consider $N = \prod_{i=1}^{n} p_i + 1$, which by Euclid's argument has a

prime factor, which we call q, such that $q \geq p_{n+1}$. Hence $p_{n+1} \leq q \leq N = \prod_{i=1}^{n} p + i + 1 \leq 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{n-1}} + 1 = 2^{2^0+2^1+\cdots 2^{n-1}} + 1 = 2^{2^n-1} + 1 \leq 2^{2^n-1} + 2^{2^n-1} = 2^{2^n}$, as required.

Now, given $x \geq 2$ let k be the integer satisfying $2^{2^{k-1}} \leq x < 2^{2^k}$, noting that $k \leq 1$. Since $p_k \leq 2^{2^{k-1}}$, we have $p_k \leq x$, so $\pi(x) \geq k$. Now, we solve for k as follows: $x < 2^{2^k} \implies \log(x) < 2^k \log(2) < 2^k \implies \log(\log(x)) < k \log(2) < k \leq \pi(x)$, hence $\pi(x)$ is bounded below by $\log(\log(x))$

□

Proposition 17. *For $x \geq 2$, $\pi(x) > \frac{\log(x)}{2\log(2)}$*

Proof. Suppose $\pi(x) = k$ and let p_1, p_2, ..., p_k be the firs k prime numbers. Let n be an integer in $[1, x]$. For each n we can uniquely write $n = a^2 b$, where a, $b \in \mathbb{N}$ and b is "square-free" (not divisible by the square of a prime). Now, $a^2 \leq n \leq x$, so $a \leq \sqrt{x}$, so there are at most $\sqrt{x}$ choices for a. Also, $b \leq n \leq x$, so b is a product of the first k prime numbers, where each prime can only appear at most once. So, the number of choices for b are at most 2^k. So, the number of choices for (a, b) is smaller than or equal to $\sqrt{x} \cdot 2^k$. Hence, $\sqrt{x} \cdot 2^n \geq x$. This results in $2^k \geq \sqrt{x}$, so $k \log(2) \geq \frac{1}{2} \log(x)$, so $\pi(x) = k \geq \frac{\log(x)}{2\log(2)}$.

□

As an example of the efficiency of this bound, we test it with $x = 10^21$. We know from exterior results that $\pi(x) = 21,127,269,486,018,731,928 \approx 2.1 \cdot 10^19$. Our bounds produce the numbers 3.878 and 34.9, respectively (very weak results). The prime number theorem yields approximately $20,680,689,614,440,563,221$, or $2.1 \cdot 10^19$, a much better estimate. Assuming the Riemann Hypothesis, we can use the logarithmic integral to calculate the estimate $21,127,269,486,616,126,181.3\ldots$, clearly a much better estimate, but, alas, the hypothesis remains unproven.

Congruences

Definition. *Let $n \in \mathbb{N}$ and a, $b \in \mathbb{Z}$. If $n|(a-b$, then we say that a is congruent to b modulo n, and we write $a \equiv b \pmod{n}$. If $n \nmid (a-b)$, then we write $a \not\equiv b \pmod{n}$. Here, n is the modulus.*

Note that $a \equiv b \pmod{n}$ if and only if $a = b + kn$ for some $k \in \mathbb{Z}$. The following are properties of congruences:

- $a \equiv a \pmod{n}$ (reflexivity)
- $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$ (symmetry)
- $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$ (transitivity)
- $a \equiv a' \pmod{n} \wedge b \equiv b' \pmod{n} \implies a + b \equiv a' + b' \pmod{n}$
- $a \equiv a' \pmod{n} \wedge b \equiv b' \pmod{n} \implies ab \equiv a'b' \pmod{n}$
- $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$, for $k \in \mathbb{N}$
- $ac \equiv bc \pmod{n} \wedge \gcd(c, n) = 1 \implies a \equiv c \pmod{n}$

Proposition 18. *Let $n \in \mathbb{N}$, and a, $b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b leave the same remainder when divided by n.*

Proof. Long division gives $a = q_1 n + r_1$, where $0 \leq r_1 < n$ and $b = q_2 n + r_2$, where $0 \leq r_2 < n$. Then $a \equiv r_1 \pmod{n}$ and $b \equiv r_2 \pmod{n}$. Since $a \equiv b \pmod{n}$, we have $r_1 \equiv r_2 \pmod{n}$ so $n|(r_2 - r_1)$. Since $-n < r_2 - r_1 < n$, we have $r_2 - r_1 = 0$, so $r_1 = r_2$.

On the other hand, if $r_1 = r_2$, then $r_1 \equiv r_2 \pmod{n}$, so $a \equiv r_1 \equiv r_2 \equiv b \pmod{n}$, so $a \equiv b \pmod{n}$.

□

Note that each $a \in \mathbb{Z}$ is congruent to exactly one number in the range $[0, n-1]$. If $a \equiv r \pmod{n}$, where $0 \leq r \leq n-1$, then r is the reduction of a modulo n, which we write $r = a \bmod n$.

Example: What is the remainder of $a = 25^171 \cdot 8^2 + 26^1991$ when divided by 13? We know that $26 \equiv 0 \pmod{1)3}$, and so we have that $26^1991 \equiv 0 \pmod{1)3}$. We also have that $8^2 = 64 \equiv 12 \pmod{1)3}$. And finally, we can see that $25 \equiv 12 \equiv -1 \pmod{1)3}$, so $25^171 \equiv (-1)^171 \equiv (-1) \pmod{1)3}$. Putting it all together yields $a \equiv (-1)(12) + (0) \equiv 1 \pmod{1)3}$.

Proposition 19. *If p is prime, and $a \in \mathbb{Z}$ with $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Define a function $f : [0, p-1] \to [0, p-1]$ by $f(x) = ax \mod p$. We want to show the function is one-to-one (injective). Suppose $f(x) = f(y)$, the by the definition of f, $(ax \mod p) = (ay \mod p)$, hence $ax \equiv ay \pmod{p}$. Since p is prime and $p \nmid a$, then $\gcd(a, p) = 1$, thus, we use the cancellation law and we have that $a \equiv y \pmod{p}$, and since both x and y are in $[0, p-1]$, we must have $x = y$.

We have that $f(0) = 0$, hence f is a bijection from $[1, p-1]$ to $[0, p-1]$. So, the numbers $\{f(1), f(2), \ldots, f(p-1)\}$ are just a rearrangement of the integers in $[1, p-1]$. Hence, $f(1) \cdot f(2) \cdots f(p-1) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$. Hence, $a \cdot 2a \cdots a(p-1) \equiv 1 \cdot 2 \cdots (p-1)$, so $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$. Since $\gcd((p-1)!, p) = 1$, we have that $a^{p-1} \equiv 1 \pmod{p}$.

□

Corollary. *If p is prime and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$*

Proof. If $p \nmid a$, then FlT tells us that $a^{p-1} \equiv 1 \pmod{p}$, so $a^p \equiv a \pmod{p}$. Otherwise, if $p|a$, then $a^p \equiv 0 \equiv a \pmod{p}$.

□

Example: Find the last 2 digits of $a = 252687^{169363^23315}$. We need to find $a \mod 100$. So, $a \equiv 87^{169363^23315} \pmod{1)00}$. We can calculate that $87^{169363^23315} \equiv (-1)^{169363^23315} \equiv -1 \pmod{4}$. Now we need to find $87^{169363^23315} \pmod{2)5}$. We see that $87 \equiv 12 \pmod{2)5}$, and we have that $12^20 \equiv 1 \equiv 12^0 \pmod{2)5}$, so the powers of 12 cycle every 20 powers back to 0. So, we need $169363^23315 \mod 20$. We see that $169363 \equiv 63 \pmod{1)00}$, and so $169363 \equiv 3 \pmod{2)0}$. Hence, $169363^23315 \equiv 3^23315 \pmod{2)0}$. We now have that $3^4 \equiv 81 \equiv 1 \pmod{2)0}$, so $3^23315 \equiv 3^{23315 \bmod 4} \equiv 27 \equiv 7 \pmod{2)0}$. Finally, $87^{169363^23315} \equiv 12^7 \equiv 8 \pmod{2)5}$, and combining with the other result we have that $252687^{169363^23315} \equiv 83 \pmod{1)00}$, so the last two digits of a are 8 and 3.

To explain some of the properties of congruences, we now discuss some properties of abstract algebra.

Definition. *Let S be a set. A relation on S is a subset $R \subseteq S \times S$. If $(a, b) \in R$, then we write aRb, and otherwise we write $a \not R b$*

Definition. *A relation R on S is an equivalence relation if for all a, b, $c \in S$:*

- *aRa (reflexivity)*
- *$aRb \implies bRa$ (symmetry)*
- *$aRb \wedge bRc \implies aRc$ (transitivity)*

For example, equality ($a = b$) and congruence modulo n ($a \equiv b \pmod{n}$) are equivalence relations, while divisibility ($a|b$) is not an equivalence relation, but still a relation.

Definition. *Let R be an equivalence relation on S, and let $a \in S$. The equivalence class of a is $[a] = \{x \in S \mid xRa\}$*

In particular, consider the equivalence relation "congruence modulo 4". Then we have that $[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$, $[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$, $[2] = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$, and $[3] = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$. These sets cover all the integers, and we can see that we have things such as $[4] = [0]$ and $[5] = [1]$. Also, the sets are all disjoint; that is, they share no elements. This leads us to the following results:

Proposition 20. *Let R be an equivalence relation on S. Let a, $b \in S$. Then we have that:*

(1) *$a \in [a]$ (obvious since aRa by reflexivity)*
(2) *If $a \not R b$, then $[a] \cap [b] = \emptyset$*
(3) *$[a] = [b]$ if and only if aRb*

Proof. Since (1) is obvious, we ommit the proof. To prove (2), suppose $x \in [a]$ and $x \in [b]$. Then xRa and xRb. By symmetry and transitivity, then aRb, which is a contradiction, so there can be no such x, and so $[a] \cap [b] = \emptyset$. Finally, for (3), if $a \not R b$, then $[a] \cap [b] = \emptyset$, so $[a] \neq [b]$. Now, if aRb, then let $x \in [a]$. This means xRa, and by transitivity xRb, so $x \in [b]$. So we have $[a] \subseteq [b]$. Similarly, $[b] \subseteq [a]$, so $[a] = [b]$.

□

Definition. *Let $n \geq 1$. The integers modulo n, written $\mathbb{Z}n$, is the set of all equivalence classes of the relation of congruence modulo n. These equivalence classes are called congruence classes.*

This definition implies that $\mathbb{Z}n = \{[1], [2], [3], \ldots, [n-1]\}$. Now, let's define addition and multiplication on the elements of $\mathbb{Z}n$ by $[a] + [b] = [a + b]$ and $[a][b] = [a \cdot b]$. We must check that these operations are well defined. If $[a] = [a']$ and $[b] = [b']$ then $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, so $a + b \equiv a' + b' \pmod{n}$, and so $[a + b] = [a' + b']$, which implies that $[a] + [b] = [a'] + [b']$ by the way we defined addition. Hence, addition is well-defined. The proof for multiplication is similar.

Proposition 21. *Let $n \geq 1$. Then $\mathbb{Z}n$ is a (finite) commutative ring.*

The proof is clear by showing that the axioms for commutative rings hold in the set $\mathbb{Z}n$. Most of them are inherited from $\mathbb{Z}$

Proposition 22. *Let $n \geq 1$. Then $\mathbb{Z}n$ is a (finite) field if and only if n is prime.*

Proof. Suppose n is prime. then $[0] \neq [1]$, and so the multiplicative and additive indentities are distinct. Now, let $[a] \in \mathbb{Z}$, with $[a] \neq [0]$. Then $a \not\equiv 0 \pmod{n}$, so by Fermat's Little Theorem $a^{n-1} \equiv 1 \pmod{n}$. So, $a \cdot a^{n-2} \equiv 1 \pmod{n}$ and $[a][a^{n-2}] = 1$, so the inverse of $[a]$ is $[a^{n-2}]$, so multiplicative inverses exist. Hence, $\mathbb{Z}n$ is a field.

On the other hand, suppose n is composite, say $n = ab$ with $1 < a,\ b < n$. Suppose $[a][x] = 1$. Then $[ax] = 1$, so $ax \equiv 1 \pmod{n}$, and we can write $ax + cn = 1$ for some $c \in \mathbb{Z}$. This would imply that $\gcd(a, n) = 1$, which contradicts the fact that $a|n$ and $1 < a < n$. We also have $a \notin [0]$, since $1 < a < n$, so we have a non-zero element with no inverse, so $\mathbb{Z}n$ is not a field

□

Proposition 23. *$[a] \in \mathbb{Z}n$ has a multiplicative inverse if and only if $\gcd(a, n) = 1$.*

Proof. If $[a]^{-1}$ exists, then there is a solution to $[a][x] = [1]$. This is equivalent to $ax \equiv 1 \pmod{n}$. Thus, $1 = ax + by$ for some $y \in \mathbb{Z}$, thus, by the GCDCT, we have that $\gcd(a, n) = 1$. The other direction follows immediately from this result by finding a soltuion to $ax + ny = 1$ with the EEA.

□

Definition. *The order of a finite field is the number of elements in the field.*

We have constructed finite fields of orders corresponding to the prime numbers. As for the other numbers, there are finite fields of orders equal to the power of strictly one prime, which we will later study as modular polynomials, but there are no finite fields whose order is a number divisible by distinct primes.

Proposition 24. *The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $\gcd(a, n)|b$*

Proof. This congruence has a solution if and only if $ax + ny = b$ has a solution, and by the Linear Diophantine Equation theorems, this has a solution if and only if $\gcd(a, n)|b$. □

Proposition 25. *If $\gcd(a, n)|b$, and x_0 is a solution to $ax \equiv b \pmod{n}$, then the complete solution is $x \equiv x_0,\ x_0 + n',\ x_0 + 2n',\ \ldots,\ x_0 + (d-1)n' \pmod{n}$, where $d = \gcd(a, n)$ and $n' = \frac{n}{d}$.*

Proof. Let $y_0 \in \mathbb{Z}$ such that $ax_0 + ny_0 = b$ Then the complete solution to this Diophantine equation is $x = x_0 + kn'$, $y = y_0 - kn'$, where $k \in \mathbb{Z}$, $n' = \frac{n}{d}$. So, the complete integer solution to $ax \equiv b \pmod{n}$ is $x = x_0 + kn'$, for $k \in \mathbb{Z}$. So, $x \equiv x_0,\ x_0 + n',\ x_0 + 2n',\ \ldots,\ x_0 + (d-1)n' \pmod{n}$ are indeed solutions to $ax \equiv b \pmod{n}$. No 2 solutions in this set are congruent in modulo n, because if $x_0 + rn' \equiv x_0 + sn' \pmod{n}$, where $0 \leq r,\ s \leq d-1$, then $n|(r-s)n'$, so $d|(r-s)$, so $r = s$. Now, if $x = x_0 + kn'$ is a solution, then we can write $k = qd + r$, where $0 \leq r \leq d-1$. Then $x = x_0 + qdn' + rn' = x_0 + qn + rn' \equiv x_0 + rn' \pmod{n}$, which is in the set of solutions we described, indeed making it the complete solution.

□

Example: We solve $217x \equiv 1260 \pmod{2}261$. We first find if there is an integer solution to the equation $217x + 2261y = 1260$. We see that $\gcd(217, 2261) = 7$, and since $7|1260$ there must be a solution. We find one such solution to be $(-125 \times 180, 12 \times 180)$. So, a solution to the linear congruence is $x \equiv -125 \times 180 \equiv 110 \pmod{2}261$. We now find the complete solution, which, by the theorem above, is $x \equiv 110,\ 433,\ 750,\ 1079,\ 1402,\ 1725,\ 2048 \pmod{2}261$. This can be more compactly written as $x \equiv 110 \pmod{3}23$.

The following theorem is presented without proof for the midterm practice problems

Proposition 26. (Wilson's Theorem)
The number p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

Proposition 27. (Chinese Remainder Theorem)
Let $m,\ n \in N$, and $a,\ b \in \mathbb{Z}$, with $\gcd(m, n) = 1$, then the simultaneous congruences

$$\begin{cases} x & \equiv a \pmod{m} \\ x & \equiv b \pmod{n} \end{cases}$$

has a solution. If $x = x_0$ is a solution, then the complete solution is $x \equiv x_0 \pmod{mn}$

Proof. The complete solution to $x \equiv a \pmod{m}$ is $x = a + my$, for $y \in \mathbb{Z}$. These x's also satisfy $x \equiv b \pmod{n}$ if and only if $a + my \equiv b \pmod{n}$, or $my \equiv b - a \pmod{n}$. Since $\gcd(m, n) = 1|(b - a)$, there exists a solution $y = y_0$. The complete solution is $y = y_0 + kn$, for $k \in \mathbb{Z}$. Hence, the complete solution to the simultaneous congruences is $x = a + m(y_0 + kn) = a + my_0 + kmn = x_0 + kmn$. Thus, $x \equiv x_0 \pmod{m}n$.

□

Example: We wish to solve $x^2 + 8x + 15 \equiv 0 \pmod{52}$. If x_0 is a solution, then all $x \equiv x_0 \pmod{52}$ are also a solution, so we restrict our search for a solution to $x \in \{0,\ 1,\ 2, \ldots,\ 51\}$. We factor to obtain $(x + 5)(x + 3) \equiv 0 \pmod{52}$. We know that this can be solved by $x \equiv -5,\ -3 \equiv 47,\ 49 \pmod{5}2$, so 47 and 49 are solutions, but these do not yield the full solution set. Instead we consider the two following equations, which provide an equivalent system:

$$\begin{cases} x^2 + 8x + 15 & \equiv 0 \pmod{13} \\ x^2 + 8x + 15 & \equiv 0 \pmod{4} \end{cases}$$

The solutions to $x^2 + 8x + 15 \equiv x^2 + 3 \equiv 0 \pmod{4}$ are $x \equiv 1,\ 3 \pmod{4}$. The solutions to $x^2 + 8x + 15 \equiv 0 \pmod{13}$ are solutions to $(x+5)(x+3) \pmod{1}3$, and since 13 is prime then $x \equiv -3,\ -5 \pmod{13} \implies x \equiv 10,\ 8 \pmod{13}$. So the solutions to the original equations obey at least one of the following:

- $x \equiv 1 \pmod{4}$ and $x \equiv 8 \pmod{13}$
- $x \equiv 1 \pmod{4}$ and $x \equiv 10 \pmod{13}$
- $x \equiv 3 \pmod{4}$ and $x \equiv 8 \pmod{13}$
- $x \equiv 3 \pmod{4}$ and $x \equiv 10 \pmod{13}$

The solutions to these systems, by the Chinese Remainder Theorem, are $x \equiv 21,\ 49,\ 47,\ 23 \pmod{52}$, so these are the solutions to the original quadratic equation.

Proposition 28. *Let a_1, a_2, ..., $a_k \in \mathbb{Z}$ and n_1, n_2, ..., $n_k \in \mathbb{N}$ with n_1, n_2, ..., n_k being pairwise relatively prime. Then the k simultaneous congruences defined by $(x \equiv a_i \pmod{n_i})_{i=1}^k$ has a solution. Moreover, if x_0 is a solution, then the complete solution is $x \equiv x_0 \pmod{\prod_{i=1}^k n_i}$.*

The proof follows by induction.

Proposition 29. (Generalization of CRT)
Let $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{Z}$. Then if $a \equiv b \pmod{\gcd(a,b)}$ then simultaneous congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ have a solution. Moreover, if x_0 is one solution, then $x \equiv x_0 \pmod{\operatorname{lcm}(m,n)}$.

Proof. The solution to $x \equiv a \pmod{m}$ is $x = a + my$, for $y \in \mathbb{Z}$. Substituting into the other congruence yields $my \equiv b - a \pmod{n}$, which we know has a solution if and only if $\gcd(m,n)|(b-a)$, which means $a \equiv b \pmod{\gcd(m,n)}$, as given in the hypothesis. The complete solution to $my \equiv b-a \pmod{n}$ is $y \equiv y_0 \pmod{\frac{n}{d}}$, where $d = \gcd(m,n)$ and y_0 is a particular solution. Thus, $y = y_0 + k\frac{n}{d}$, so $x = a+my = a+m(y_0+k\frac{n}{d} = a+my_0+k\frac{mn}{d} = x_0 + k\frac{mn}{d}$, so $x \equiv x_0 \pmod{\frac{mn}{d}}$.

□

4. Algorithmic Number Theory

From our knowledge we have developed, we know that every number larger than or equal to 2 has a unique prime factorization (by the Fundamental Theorem of Arithmetic). This arises the following questions:

- Given $n \geq 2$, can we find its prime factorization efficiently?
- Given $n \geq 2$, how do we efficiently determine if n is prime or composite?
- Is Euclid's Aglroithm efficient?

We wish to be able to answer these questions, so we begin by setting some definitions.

Basic definitions from complexity theory

Informally, an algorithm is a "well-defined computational procedure" which takes a variable input and eventually halts with some output. More precisely, algorithm can be taken to mean a Turing machine. Intuitively, an algorithm can just be represented by a computer program, but the more proper definition defines it using the properties of a Turing machine.

The input size of any algorithm is the number of bits (in binary) needed to write down or represent the input (binary will be assumed from now on as the standard representation for numbers as input in an algorithm, equating it with the common programming application). If $n \geq 2$, it's binary representation is $n = a_{k-1}2^{k-1} + \cdots + a_2 2^2 + a_1 2^2 + a_0$, where $a_i \in \{0,1\}$, and $a_{k-1} = 1$ (to make the representation unique). For example, $1153 = 2^10 + 2^7 + 1 = 10010000001_2$. The bitlength of n is k, the number of digits, and in general $k = \lfloor \log_2(n) \rfloor + 1$.

The (worst case) running time of an algorithm is an upper bound, as a function of the input's size, on the number of basic operations the algorithm takes for any input of a given size. In this course, a basic operation is a "bit operation", ie. an operation involving a "small" number of bits. For example, when we add numbers in binary, the addition of

individual digits can be defined to be one bit operation, so the upper bound on the number of bit operations is k, $2k$, or $3k$, depending on what we consider to be a bit operation (is adding the carry digit an operation? Writing down the result of a sum?). To avoid these constant multipliers, we use the following notation:

Definition. *Let f, $g : \mathbb{N} \to \mathbb{R}_{>0}$. Then $f = O(g)$ means that there is some $c > 0$ and $n_0 \in \mathbb{N}$ such that $f(n) \leq cg(n)$ for all $n \geq n_0$.*

For example, $75n^3 + 10000n^2 + 16$ is equal to $O(n^4)$. More interestingly, it is equal to $O(n^3)$, since the $75n^3$ eventually dominates the value of the expression, but it is not equal to $O(n^2)$, since the expression willalways overtake any quadratic at some point. We can now use our notation to see that the addition algorithm takes $O(k)$ bit operations. Notice that there is no faster algorithm since we must at least read in each of the k digits, and this suffices as proof that there is no faster algorithm. Most algorithm's efficiency is not this easy to prove. For multiplying k digit numbers together, we can then see that the run time is $O(k^2)$, using our naive addition of integers by digits. Obviously, integer multiplication has a lower limit of $O(k)$, but no better lower bound is known. The second best lower bound known is an algorithm running at $O(k \log(k) \log(\log(k)))$, and the best one has an expression too complicated to write here.

Division similarly require repeated subtraction, so it is also of $O(k^2)$ running time.

We summarize these and other results in the table below, for integers a and b of bitlength k:

Operation	Running Time of Simple Algorithm
$a + b$	$O(k)$
$a - b$	$O(k)$
$a \cdot b$	$O(k^2)$
$a = q + br$, $0 \leq r < b$	$O(k^2)$

Now, we consider factoring of a number by trial division. We need to attempt to divide the number n by any number smaller tha $\sqrt{n}$ to get all divisors, and since each division takes $O(k^2)$ time, then factoring by trial division takes $O(\sqrt{n}k^2)$ time. Since $\sqrt{n}$ is bigger than $2^{\frac{k}{2}}$, then factoring by trial division takes $O(2^{\frac{k}{2}}k^2)$. Notice that this increases very rapidly for larger values of k, so we do not consider this to be efficient when compared to the other algorithms described above. This prompts us to define efficiency in running time.

Definition. *An algorithm is a polynomial-time algorithm if it's running time is of the form $O(k^c)$, where k is the input size and c is a constant. Otherwise, it is an exponential-time algorithm. Informally, we consider polynomial-time algorithms to be efficient, and exponential-time algorithms to be inefficient.*

We are now ready to analyze whether Euclid's algorithm is actually efficient or not.

Proposition 30. *Euclid's algorithm has at most $2k$ division steps. Also, Euclid's algorithm takes $O(k^3)$ time.*

Proof. Consider 3 consecutive divisions:

$$r_{j-2} = q_j r_{j-1} + r_j,\ 0 < r_j < r_{j-1}$$
$$r_{j-1} = q_{j+1} r_j + r_{j+1},\ 0 < r_{j+1} < r_j$$
$$r_j = q_{j+2} r_{j+1} + r_{j+2},\ 0 < r_{j+2} < r_{j+1}$$

Suppose that $r_{j+1} < \frac{r_j}{2}$. Then $r_{j+2} < \frac{r_j}{2}$. Suppose that $r_{j+1} > \frac{r_j}{2}$. Then $q_{j+2} = 1$, so $r_j = r_{j+1} + r_{j+2}$, and so $r_{j+2} = r_j + r_{j+1} < \frac{r_j}{2}$. Hence, $r_{j+2} < \frac{r_j}{2}$, and thus the bitlength of r_{j+2} is at least one less than the bitlength of r_j. Since r_1 has bitlength smaller than or equal to k, there are at most $2k$ divisions before a 0 remainder is reached. Thus, Euclid's algorithm takes $O(2k \cdot k^2) = O(k^3)$ time.

□

Recall that factoring by trial division has a running time of $O(2^{\frac{k}{2}} k^2)$. The fastest known factoring algorithm has run time $O(2^{k^{\frac{1}{3}}})$ (Number Field Sieve, 1990), which is much faster but still not polynomial. This raises a few questions: Is there a faster integer factorization algorithm? Is there or is there not a polynomial time (polytime) factoring algorithm?

Notice that a quantum computer breaks these rules; there is a factoring algorithm that runs in $O(k^3)$ on quantum computers. In 2012, researchers at UCSB built a quantum computer to factor the number 15. The machine works accurately 48% of the time. These machines are not yet scalable, though, so larger numbers are still not feasible to factor.

Primality Testing

Given a number $n \geq 2$, how do we efficiently decide if it is prime or composite? Some properties separate composites from primes:

- n is composite if and only if n has a (prime) factor m, with $2 \leq m \leq \sqrt{n}$
- n is prime if and only if $\sum_{m=q}^{\infty} \left(\lfloor \frac{n}{m} \rfloor - \lfloor \frac{n}{m-1} \rfloor \right) = 2$
- n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$
- n is prime and $n \nmid a$, then $a^{n-1} \equiv 1 \pmod{n}$. If n is composite, and $n \nmid a$, this is generally false.

This last property leads us to the Fermat Test for primality, which is described as follows:

(1) Repeat ℓ times:
(2) Select a randomly from $[1, n-1]$
(3) Compute $t = a^{n-1}$
(4) If $t \neq 1$, then output "Composite"
(5) GOTO 1
(6) Output "Probably Prime"

We now analyze some questions that arise to this algorithm:

(1) Efficiency: Recall $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$. For convenience, we write $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Now, suppose n is k bits long, and that $a,\ b,\ m \in [0, n-1]$.

The standard running time of $(a+b) \mod n$ is $O(k)$, since we can avoid the division by subtracting n once. Similarly, $(a-b) \mod n$ is $O(k)$, and $a \cdot b \mod n$ is $O(k^2)$. These are all polytime, but now we need to know whether exponentiation and the subsequent modulus are efficient. Doing the repeated multiplication and then the modulus is very inefficient, but we can devise an algorithm that supplies $a^m \mod n$ in time $O(k^3)$. We use the repeated square-and-multiply method for modular exponentiation, as follows:

(a) Write $m = \sum_{i=0}^{k-1} m_i 2^i$, with $m_i \in \{0, 1\}$

(b) Then $a^m = a^{\sum_{i=0}^{k-1} m_i 2^i} = \prod_{i=0}^{k-1} a^{m_i 2^i} = \prod_{i=0, m_i=1}^{k-1} a^{2^i}$. Hence, compute $a^2 \mod n$, $a^4 \mod n$, ..., $a^{2^{k-1}} \mod n$, and multiply the numbers $\mod n$ for which $m_i = 1$

The run-time of this algorithm is k multiplications plus k squaring, which equates to $2k$ multiplications, which are each run in $O(k^2)$ time, yielding a total run-time of $O(k^3)$. Hence, Fermat's primality test has a running time of $O(\ell k^3) = O(k^3)$, as long as ℓ is constant.

(2) Correctness: If $a \in [1, n-1]$ and $a^{n-1} \not\equiv 1 \pmod{n}$, then a is called a Fermat witness for the compositeness of n. Otherwise, if $a \in [1, n-1]$ and $a^{n-1} \equiv 1 \pmod{n}$, the number a is called a Fermat liar for n. For Fermat's primality test to work, we must have significantly more witnesses than liars for most composite numbers n.

If $a \in [1, n-1]$ and $\gcd(a, n) > 1$, then we know that $a^{n-1} \not\equiv 1 \pmod{n}$, so a is a Fermat witness for n. If n is hard to factor (eg, n is a product of two large primes), then the witnesses are rare.

Definition. $\mathbb{Z}_n^* = \{1 \le a \le n-1 \mid \gcd(a, n) = 1\}$. *We can prove that if* $b, c \in \mathbb{Z}_n^*$, *then* $bc \in \mathbb{Z}_n^*$.

Proposition 31. *Suppose* n *is composite, and suppose that* n *has at least one Fermat witness in* $\mathbb{Z}_n^*$, *which we call* b. *Then at least half of all numbers in* $\mathbb{Z}_n^*$ *are witnesses for* n.

Proof. Let $a_1, a_2, \ldots, a_s$ be the set of all Fermat liars of n in $\mathbb{Z}_n^*$. We claim that $b_i \equiv ba_i \pmod{n}$ for $1 \le i \le s$ are Fermat witnesses for n. This is true because $\gcd(b_i, n) = 1$ and $b^{n-1} \equiv (ba_i)^{n-1} \equiv b^{n-1} a_i^{n-1} \equiv b^{n-1} \not\equiv 1 \pmod{n}$. Moreover, if $ba_i \equiv ba_j \pmod{n}$, then $a_i \equiv a_j \pmod{n}$, since we can cancel out b because $\gcd(b, n) = 1$, and this implies $i = j$. Hence, there are at least s Fermat witnesses for n.

□

Definition. *An odd composite number* n *is Carmichael if* $a^{n-1} \equiv 1 \pmod{n}$ *for all* $a \in \mathbb{Z}_n^*$.

For example, 561 is a Carmichael number. This can be easily checked; if we let $a \in \mathbb{Z}_{561}^*$, then since $561 = 3 \cdot 11 \cdot 17$ we have that $\gcd(a, 3) = 1$. Thus, we can write $a^{560} \equiv (a^2)^{280} \equiv 1 \pmod{3}$. Similarily, we can see that $a^{560} \equiv 1 \pmod{11}$ and $a^{560} \equiv 1 \pmod{17}$, so $a^{560} \equiv 1 \pmod{561}$.

Proof. There are infintely many Carmichael numbers

□

Proposition 32. *A number n is Carmichael if and only if n is square-free and $n-1$ is divisible by each prime divisor of n minus 1.*

The proof of $\leftarrow$ is provided by the example above. The proof for $\rightarrow$ requires techniques unavailable to us now.

These two results tell us that if Fermat's primality test outputs "Composite", then n is certainly prime, and efficiently-verifiable proof is provided. Otherwise, if it outputs "Probably Prime", then either n is prime or Carmichael, or n is composite and we only picked out Fermat liars of n, which has a probability of $p \leq \frac{1}{2^\ell}$. If $\ell = 100$, this probability is $p \leq \frac{1}{2^{100}}$, which is nearly negligible.

The "Miller-Rabir" test is a refinement of Fermat's primality test, which separates primes from Carmichael numbers (see Assignment #5). Also, if n is a non-Carmichael composite number, then it has been proven that there is a Fermat witness $a \in [1, 2(\log_e(n))^2]$ provided the Extended Riemann Hypothesis is true.

RSA encryption

We begin this topic with an introduction to cryptography. In cryptography, we usually have two parties (generally called Alice and Bob) communicating through a channel. We then copnsider the situation where Cris is trying to affect the data being sent, either by reading it, modifying it, or injecting it. The basic goals of cyptography are:

(1) Confidentiality: When Bob receives a message from Alice, he is assure that only him and Alice ca learn the contents of the message.
(2) Authentication: When Bob receives a message, supposedly from Alice, he is assured that the message indeed originated from Alice.

We will now focus on the confidentiality aspect of cryptography. For thousands of years, "symmetric-key" cryptography has been used, which basically means Alice and Bob agree on a secure key through a secure channel, and then they can communicate over the communications channel, with Bob decoding the message using the key and Alice using it to encrypt it. Theoretically, without the key, then Chris is unable to read or succesfully modify the messages. This idea is good theoretically, but it has many complications in practice (setting up secure channel, prevent decryption of message, etc).

Because of these weaknesses, a new method emerged in the 1970's: public-key encryption. In this type of encryption, Bob would send Alice a public key over an authenticated channel, which is not necessarily secret. Then Alice encodes the message using the public key and sends it to Bob. Now, Bob uses the corresponding private key, which is kept secret by Bob, to decode the message. One such method of encryption is outlined in the Rivest-Shamir-Adleman (RSA) public-key encryption scheme, described in the following steps:

(1) Key Generation: Bob selects two large primes p and q. For simplicity, we say they have the same bit-length. In this case, with modern computers and factoring algorithms, primes of at least 512 bits of length are necessary, but 1024 is preferable.

Then, Bob computes $n = pq$ and $\phi(n) = (p-1)(q-1)$. He selects an arbitrary number e such that $1 < e < \phi(n)$, with $\gcd(e, \phi(n)) = 1$. We then compute d as $d \equiv e^{-1} \pmod{\phi(n)}$. Bob's public key is then (n, e), and his private key is d.

(2) Encoding: To encrypt a message for Bob, Alice first obtains an authentic copy of Bob's public key, the numbers (n, e). Alice then represents the message as an integer m with $m \in [0, n-1]$. Then Alice computes $c = m^e \mod n$, done using the squaring and multiplying method. This number c is sent to Bob.

(3) Decryption: Bob receives c, and then he computes $r = c^d \mod n$. Then $r = m$.

We now prove the fact that $r = m$

Proposition 33. *The RSA algorithm described above produces the original message when decoded ($r \equiv c^d \equiv (m^e)^d \equiv m \pmod{n}$)*

Proof. Suppose $p|m$. Then $m \equiv 0 \pmod{p}$, so $m^{ed} \equiv \pmod{p}$. Then $m^{ed} \equiv m \pmod{p}$, and the result follows immediately.

Now suppose $p \nmid m$. Then $m^{p-1} \equiv 1 \pmod{p}$. Since $ed \equiv 1 \pmod{\phi(n)}$, we have $ed = 1 + k(p-1)(q-1)$ for some $k \in \mathbb{N}$. Then raising $m^{p-1} \equiv 1 \pmod{p}$ to the power of $k(q-1)$ gives $m^{k(p-1)(q-1)} \equiv 1 \pmod{p} \implies m^{ed} \equiv m \pmod{p}$. Similarly, $m^e d \equiv m \pmod{q}$, and since $\gcd(p, q) = 1$, then $m^e d \equiv m \pmod{n}$, as required.

□

A few notes on RSA follow:

A simple example is described in the handout online, and more details and exercises are shown in Assignment #5.

For any eavesdorpper ("Chris"), the goal is to compute m given c and (n, e). The only known method to solve this problem is to factor n, which has been shown already to be very difficult to accomplish in a short time-frame. So the security of RSA depends on the hardness of factoring the number n.

For the algorithm to work, it must be relatively easy to generate large primes. By the prime number theorem, we know that $\pi(x) \approx \frac{x}{\log(x)}$. For generating 512-bit primes, we see that the proportion of such numbers that are prime is $\frac{\pi(2^{512}) - \pi(2^{511}}{2^{511}} \approx \frac{1}{356}$, so expects to try about 356 random numbers until a prime is found, which can then be checked using some primality test, such as Fermat's primality test. Using several more advanced algorithms reduces the expected number of trials.

The RSA signature scheme also allows for authentification while using the RSA scheme. This is examined in detail in the handout provided in-class. To sign a message m, Bob computes $h = H(m)$, where H is a hash function. Then he computes $s \equiv h^d \pmod{n}$, which he can now send to whomever it is required as the compound message (m, s). To verify the message, Alice first obtains an authentic copy of Bob's public key. Alice then computes the hash of the message, and she accepts the message if $s^e \equiv h \pmod{n}$. This completes the signature and verification algorithm.

For internet security, some of the details are different. See the handout provided in-class for details.

Algebraic Number Theory

Definition. *Let $d \neq 1$ be a square-free integer. Then we know that $\sqrt{d} \notin \mathbb{Q}$. We define $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ and $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.*

Notice that $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Q}(\sqrt{d})$ and $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$. If $d > 1$, then $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$, while if $d < 1$, then $\mathbb{Q}(\sqrt{d}) \nsubseteq \mathbb{R}$, but we always have that $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$. If we let $r_1 + s_1\sqrt{d}$, $r_2 + s_2\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, then $r_1 + s_1\sqrt{d} = r_2 + s_2\sqrt{d}$ if and only if $r_1 = r_2$ and $s_1 = s_2$. Addition and multiplication in $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Z}[\sqrt{d}]$ are defined naturally. We see that $\mathbb{Q}(\sqrt{d})$ is also a field; most properties are inherited from the field $\mathbb{C}$, and we have multiplicative inverses for non-zero elements: $(r + s\sqrt{d})^{-1} = \frac{r - s\sqrt{d}}{r^2 - s^2 d} \in \mathbb{Q}(\sqrt{d})$.

Definition. *We say $x \in \mathbb{Z}[\sqrt{d}]$ is a unit if there is some $y \in \mathbb{Z}[\sqrt{d}]$ such that $xy = 1$.*

Definition. *Let $x = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. The conjugate of x is $\overline{x} = r - s\sqrt{d}$, and the norm of x is $N(x) = \overline{x}x = r^2 - s^2 d \in \mathbb{Q}$*

Proposition 34. *The following are properties of the norm for x, $y \in \mathbb{Q}(\sqrt{d})$:*

- *$N(x) = 0$ if and only if $x = 0$*
- *$\overline{x + y} = \overline{x} + \overline{y}$*
- *$\overline{x \cdot y} = \overline{x} \cdot \overline{y}$*
- *$N(xy) = N(x)N(y)$*

If x, $y \in \mathbb{Z}[\sqrt{d}]$, then:

- *$N(x) \in \mathbb{Z}$*
- *x is a unit if and only if $N(x) = \pm 1$*

With these properties, we can see that $Z[\sqrt{d}]$ is not a field. However, we can check the following result.

Proposition 35. *$\mathbb{Z}[\sqrt{d}]$ is a commutative ring.*

Definition. *Let x, $y \in \mathbb{Z}[\sqrt{d}]$. We say $x|y$ if there is some $z \in \mathbb{Z}[\sqrt{d}]$ such that $y = xz$.*

Proposition 36. (Propoerties of Divisibility)

- $x|x$
- $x|y \wedge y|z \implies x|z$
- $x|y \wedge x|z \implies \forall(a, b \in \mathbb{Z}[\sqrt{d}])x|ay + bz$
- $1|x$
- $x|0$
- $x|y \implies N(x)|N(y)$ *(easy to prove since $x = yz \implies N(x) = N(yz) = N(y)N(z)$)*

The last property is usefule for proving non-divisibility. Notice, though, that the converse is not usually true.

Definition. *A number $x \in \mathbb{Z}[\sqrt{d}]$ is called a prime if x is not a unit and if $x = yz$, with y, $z \in \mathbb{Z}[\sqrt{d}]$, then either y or z is a unit.*

Proposition 37. *Let $x \in \mathbb{Z}[\sqrt{d}]$. If $|N(x)|$ is prime (in the naturals), then x is prime (in $\mathbb{Z}[\sqrt{d}]$).*

Proof. Since $|N(x)|$ is prime, we have $N(x) \neq \pm 1$, and so x is not a unit. Suppose $x = yz$, then $N(x) = N(yz) = N(y)N(z)$, so $N(y) = \pm 1$ or $N(z) = \pm 1$, since $N(x)$ is prime. Thus, x is prime.

□

This last condition is sufficient, but not necessary. For instance, consider the number 5. We have that $N(5) = 25$, so the norm is not prime. If $5 = yz$ with y, $x \in \mathbb{Z}[\sqrt{2}]$ are not units, then $25 = N(5) = N(y)N(z) \implies N(y) = \pm 5$. Then $N(y) = a^2 - 2b^2 = \pm 5$, so $a - 2b^2 \equiv 0 \pmod 5 \implies a^2 = 2b^2 \pmod 5$. But the square modulo 5 are 0, 1, and 4, so the only solution to this is $a \equiv 0 \pmod 5$. Hence $25|a$ and $25|b^2$, so $25|a^2 - 2b^2 = \pm 5$, which is impossible. Hence 5 is prime in $\mathbb{Z}[\sqrt{2}]$.

We say that $\mathbb{Z}[\sqrt{d}]$ is a quadratic number domain. A commutative ring R is an integral domain if $1 \neq 0$ and $a \cdot b = 0 \implies a = 0 \vee b = 0$, where a, $b \in R$.

Example: (Fermat) Find all integer solutions to $y^2 + 2 = x^3$.

Solution: (Euler) Note that y must be odd, otherwise $2|x$ and reducing the equation modulo 4 yields $2 \equiv 0 \pmod 4$, which is impossible. We rewrite the equation as $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$, where x, $y \in \mathbb{Z}$. Now, we are working in $\mathbb{Z}[\sqrt{-2}]$.

We claim that $y + \sqrt{-2}$ and $y - \sqrt{-2}$ have no non-trivial common divisors. Suppose that $c + d\sqrt{-2}|y + \sqrt{-2}$ and $c - d\sqrt{-2}|y - \sqrt{-2}$. Hence, $c + d\sqrt{-2}|2y$ and $c + d\sqrt{-2}|2\sqrt{-2}$. So, $c^2 + 2d^2|4y^2$ and $c^2 + 2d^2|8$ (taking norms). Since y is odd and $c^2 + 2d^2|8$, the equation $c^2 + 2d^2|4y^2$ tells us that $c^2 + 2d^2|4$. If $c = 0$, then $d = \pm 1$; if $c = \pm 1$, then $d = 0$; if $c = \pm 2$, then $d = 0$. In the second case, then $c + d\sqrt{-2}$ is a unit, so we ignore it. In the first case, then $\pm\sqrt{-2}(a + b\sqrt{-2}) = y + \sqrt{-2} \implies \pm 2b \pm a\sqrt{-2} = y + \sqrt{-2}$, which would imply y is even, a contradiction. The last case gives us a similar contradiction, so $y + \sqrt{-2}$ and $y - \sqrt{-2}$ have no common factors.

The lack of common factors tell us that $y + \sqrt{-2}$ and $y - \sqrt{-2}$ must be cubes, say $y + \sqrt{-2} = (a + b\sqrt{-2})^3 = a^3 + 3a^2b\sqrt{-2} - 6ab^2 - 2b^3\sqrt{-2} = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}$. Equating coefficinets tells us that $1 = b(3a^2 - 2b^2)$, so $b = 1$ and $a = \pm 1$ ($b = -1$ yields no integer solutions for a). Thus, $y = a^3 - 6ab^2$ gives $y = \pm 5$, and so $x = 3$.

This solution works very well for $d = 2$, but we showed in class it does not work for $d = 47$. We found one solution using this method, but we were able to calculate a smaller solution that was not found by this method. This is due to the assumption that $\mathbb{Z}[\sqrt{d}]$ has unique factorization when we say that $y + \sqrt{-2}$ is a cube, which is not true for all d (it is for 2). This error has been mad by many great mathematicians of the past, most notably Lame and Cauchy, whose fallacious proofs of Fermat's Last Theorem assumed unique factorization in the ring $\mathbb{Z}[e^{\frac{2i\pi}{n}}]$. Thus, we wonder when there are unique factorizations, or if they can even exist at all.

Proposition 38. (Existence of factorizations)

Every non-zero number $x \in \mathbb{Z}[\sqrt{d}]$ can be written as the product of a unit and finitely many primes in $\mathbb{Z}[\sqrt{d}]$, known as a prime factorization.

Proof. Define $S \subseteq \mathbb{Z}[\sqrt{d}]$ be the set of numbers that do not follow this property. Suppose S is non-empty. Define $T = \{|N(x)| \mid x \in S\}$. By the well-ordering theorem, there must be a smallest element in T, say $|N(x_0)|$ where $x_0 \in S$. Now, x_0 is not a unit nor a prime, since then it would immediately contradict the definition of S. Hence, we can write $x_0 = yz$ where y, $z \in \mathbb{Z}[\sqrt{d}]$ and neither y nor z are units. But then $|N(x_0)| = |N(y)||N(z)|$, so we have $|N(y)| < |N(x_0)|$ and $|N(z)| < |N(x_0)|$, and since y and z are non-zero, then they are not in S, and so they have a prime factorization, which we can multiply together to get a prime factorization for x_0. This contradicts the definition of x_0, so the assumption that S is non-empty must be false. Hence, all numbers have a prime factorization.

□

Before we attempt to prove uniqueness, we define some terminology.

Definition. *We say that x, $y \in \mathbb{Z}[\sqrt{d}]$ are associates if $x = uy$ for some unit $\mathbb{Z}[\sqrt{d}]$.*

Some properties of associates are as follows:

- The relation of "being an associate" is an equivalence relation on $\mathbb{Z}[\sqrt{d}]$
- If x and y are associate, then $|N(x)| = |N(y)|$
- If $x|y$, then $x|y$ for all associates z of x
- If p is prime and u is a unit, then the product is also a prime

Definition. *The commutative ring $\mathbb{Z}[\sqrt{d}]$ is a unique factorization domain (UFD) if for all non-zero $x \in \mathbb{Z}[\sqrt{d}$ the following is true:*

- *If $x = up_1 \dots p_\ell = vq_1 \dots q_k$, where u and v are units and p_i, q_j are primes, then $\ell = k$ and there is a permutation π of $\{1, 2, \dots, \ell\}$ such that $q_{\pi(i)}$ is an associate of p_i, for each $1 \leq i \leq \ell$.*

Example: $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. This is seen because $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Now, $N(2) = 4$, $N(3) = 9$, and $N(1 \pm \sqrt{-5}) = 6$, so 2 and 3 are not associate of $1 \pm \sqrt{-5}$. Also, 2 is prime because if $2 = yz$, where y and z are not units, then $4 = N(2) = N(y)N(z)$, so $N(y) = \pm 2$, but since $y = a + b\sqrt{-5}$, then its norm is $a^2 + 5b^2 = \pm 2$, which is impossible, generating a contradiction, so 2 is prime. Similarly, 3 is prime. Since $N(1 \pm \sqrt{-5}) = 6$, and there are no numbers of norm ± 2 or ± 3 in $\mathbb{Z}[\sqrt{-5}]$, then $1 \pm \sqrt{-5}$ are primes as well, so these combinations denote distinct prime factorizations of 6, so $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

We will prove soon that $\mathbb{Z}[\sqrt{-1}]$ is a UFD. The proof that $\mathbb{Z}[\sqrt{-2}]$ is a UFD is on Assignment #6, and similarly the proof that for $d < -2$ $\mathbb{Z}[\sqrt{d}]$ is not a UFD is also on Assignment #6. It is more complicated to prove for $d > 0$, although it is know that $\mathbb{Z}[\sqrt{d}]$ is a UFD for $d = 2$, 3, 6, 7, 11, 14, 19, 22, 23, 31. It is unknown if $\mathbb{Z}[\sqrt{d}]$ is a UFD for infinitely many d.

It is relatively easy to see why proving unique factorization in $\mathbb{Z}[\sqrt{d}]$ with $d > 0$ is hard. For example, take $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\sqrt{2}]$. In $\mathbb{Z}[\sqrt{-2}]$, $u = a + b\sqrt{-2}$ is a unit if and only if $N(u) = a^2 + 2b^2 = \pm 1$, and clearly the only solutions to this are $u = \pm 1$. However, in $\mathbb{Z}[\sqrt{2}]$, $u = a + b\sqrt{2}$ is a unit if and only if $N(u) = a^2 - 2b^2 = \pm 1$ (this is known as a Pell equation). Note that then $u = 1 + \sqrt{2}$ is a unit, and $u \in \mathbb{R}$ with $u > 1$, so u^n is a distinct

unit for $n \in \mathbb{Z}$. Hence, $\mathbb{Z}[\sqrt{2}]$ has infinitely many units (in fact, Dirichlet's unit theorem, which will not be proven here, tells us that all of its units are $\pm(1+\sqrt{2})^n$, for $n \in \mathbb{Z}$), which makes proving the unique factorization much harder. Special cases can be made, though, as follows:

Example: We prove that if $d \equiv 1 \pmod 4$, then $\mathbb{Z}[\sqrt{d}]$ is not a UFD. Let $d = 1 + 4k$, with $k \in \mathbb{Z}$. Then $d - 1 = 4k = 2(2k) = (-1 + \sqrt{d})(1 + \sqrt{d})$. Now, 2 is prime in $\mathbb{Z}[\sqrt{d}]$ since there are no elements of norm ± 2. This can be easily seen by reducing $a^2 - db^2 = \pm 2$ modulo 4 to see that $a^2 - b^2 \equiv \pm 2 \pmod 4$, which has no solution since the squares modulo 4 are 0 and 1. Also, $2 \nmid (1 + \sqrt{d})$, and so no associate of 2 divides $1 + \sqrt{2}$. We can show the same thing for $-1 + \sqrt{d}$, so we have one factorization with 2 as a prime factor but another one without any associate of 2 as a factor, so $d - 1$ has two different prime factorizations, and $\mathbb{Z}[\sqrt{d}]$ is not a UFD.

Definition. *We call the set $\mathbb{Z}[\sqrt{-1}]$ the Gaussian Integers, and we write them as $\mathbb{Z}[i]$. Primes in $\mathbb{Z}[i]$ are called Gaussian primes, and its units are ± 1, $\pm i$*

We want to prove unique factorization for $\mathbb{Z}[i]$, like we did for $\mathbb{Z}$. We notics that the process for proving this for $\mathbb{Z}$ started with finding the division algorithm, so we prove this for $\mathbb{Z}[i]$.

Proposition 39. *Let a, $b \in \mathbb{Z}[i]$ with $b \neq 0$. Then there are q, $r \in \mathbb{Z}[i]$ such that $a = qb + r$, with $0 \leq N(r) < N(b)$.*

Proof. We have $\frac{a}{b} = \frac{a \cdot \bar{b}}{b\bar{b}} = \frac{a \cdot \bar{b}}{N(b)} \in \mathbb{Q}(i)$. So, we can write $\frac{a}{b} = u + vi$, where u, $v \in \mathbb{Q}$. Select x, $y \in \mathbb{Z}$ with $|x - u| \leq \frac{1}{2}$ and $|y - v| \leq \frac{1}{2}$. Let $q = x + iy \in \mathbb{Z}[i]$ and $r = a - qb \in \mathbb{Z}[i]$. Then $a = qb + r$ and $N(r) = N(a - qb) = N(b(\frac{a}{b} - q)) = N(b)N(\frac{a}{b} - q) = N(b)N((u - x) + (v - y)i) = N(b)[(u - x)^2 + (v - y)^2] \leq N(b)[\frac{1}{4} + \frac{1}{4}] = \frac{1}{2}N(b) < N(b)$. Note that q and r are not necessarily unique.

□

Definition. *Let a, $b \in \mathbb{Z}[i]$. Then $d \in \mathbb{Z}[i]$ is a GCD of a and b if (1) $d|a$ and $d|b$, and (2) $\exists x$, $y \in \mathbb{Z}[i]$ with $ax + by = d$.*