Day 14

Gaussian integers and Fermat's Theorem

Lemma: The congruence $x^2 \equiv -1 \pmod{p}$ has a solution modulo a prime p if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Proof: If $p = 2$, 1 is a solution. If p is odd, and $x^2 = -1$ has a solution, then $(\mathbb{Z}/p\mathbb{Z})^\times$ has an element of order 4, so $4|(p-1)$. Notice that $(\mathbb{Z}/p\mathbb{Z})^\times$ has only two elements of order dividing 2, because of $x^2 \equiv 1 \pmod{p}$ then $p|(x^2-1)$, so $p|(x+1)(x-1)$, so either $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. If $4|(p-1)$ then let H be the Sylow 2-subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. If H were not cyclic, then there would be too many elements of order 2 in H. So H must be cyclic and therefore there is an element of order 4.

Now suppose that $p \equiv 1 \pmod{4}$. Let u be a solution to $x^2 + 1 \equiv 0 \pmod{p}$. Consider the ideal $I = (p, u+i) \subset \mathbb{Z}[i]$. This is a maximal ideal. If $\pi = a + bi$ is a generator of this ideal, then $p = x\pi$. If x were a unit, then $u + i$ would have to be a multiple of p, which it visibly isn't. Therefore $N(\pi)$ must be p.
But $N(\pi) = a^2 + b^2$, so we've found our representation.

Proposition: The ring $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean ring. In fact, the ideal $(3, 1+\sqrt{-5})$ is not principal. It is a proper ideal, because the quotient of $\mathbb{Z}[\sqrt{-5}]$ by this ideal is $\mathbb{Z}/3\mathbb{Z}$. If π were a generator of this ideal, then $3 = x\pi$ means that either $N(\pi) = 3$ or $N(\pi) = 9$. Also $(1 + 5i) = y\pi$ means that $N(\pi)$ divides 6. Since π is not a unit, $N(\pi) = 3$. But the equation $x^2 + 5y^2 = 3$ has no integer solutions, so there is no element of norm 3 in this ring.

Principal Ideal domains

Definition: An integral domain in which every ideal is principal is called a Principal Ideal Domain.

Principal ideal domains satisfy the conclusions of the Euclidean algorithm (but maybe without the algorithm).

That is, given $a, b \in R$ if R is a PID, then the ideal $(a, b) = (d)$ where d is a greatest common divisor of R, and there are x and y in R such that $ax + by = d$. The gcd d is unique up to multiplication by a unit.

Proposition: A Euclidean ring is a PID. (DF p. 281 contains a strengthening of this result, proving that an integral domain R is a PID if and only if it has a "Dedekind-Hasse" norm, which is a slightly more general type of norm that isn't necessarily positive)

Note: The converse is not true, but the question of existence of Euclidean algorithms is subtle. See Conrad's notes on the euclidean domains for a discussion. DF prove that $\mathbb{Z}[(1+\sqrt{-19})/2]$ is a PID but is not Euclidean with respect to any norm (see page 277).

Proposition: In a principal ideal domain, every nonzero prime ideal is maximal.

Proof: Suppose (p) is a prime ideal and (m) is an ideal with $(p)\subset(m)$. Then $p=mx$ for some $x\in R$. Since (p) is prime, either $m\in P$ or $x\in P$. If $m\in P$, then $(m)=(p)$. If $x\in P$, then $x=pr$ and so $p=mpr$ or $p(1-mr)=0$, meaning $mr=1$ and so m is a unit. Then $(m)=R$. So the only ideals of R containing (p) are (p) and R, and (p) is maximal. (Note: this is the ideal theoretic version of the statement that, if $p|xm$, then either $p|x$ or $p|m

Unique factorization

Key Terminology: Let R be an integral domain.

1. A non-unit element $x\in R$ is called irreducible if whenever $x=ab$ in R, either a or b is a unit.
2. A non-unit element $x\in R$ is called prime if, whenever p divides ab, either p divides a or p divides b. Equivalently, p is prime if the ideal pR is a prime ideal.
3. Two elements a and b are called associates in R if there is a unit in R such that $a=bu$.

Example: In a polynomial ring $F[x]$ over a field F, the irreducible elements are the irreducible polynomials. Every irreducible element is prime (by the Euclidean algorithm). In the ring $\mathbb{Z}[\sqrt{-5}]$ the element 2 is irreducible by not prime, since 2 divides $(1+\sqrt{-5})(1-\sqrt{-5})=6$ but does not divide either of the factors.

Lemma: If R is an integral domain, then every prime is irreducible. If R is a principal ideal domain, then the converse is true.

Proof: If p is a prime element, and $p=xy$, then either $p|x$ or $p|y$. Assume $x=pu$. Then $p=puy$ so $p(1-uy)=0$ and therefore $uy=1$ so y is a unit and p and x are associates. Similarly if pR is a prime ideal then R/pR is an integral domain, so $xy=0$ in R/pR implies either $x\in pR$ or $y\in pR$.

If R is a PID, and q is irreducible, suppose q divides xy. Let d generate the ideal (q,x). If d is a unit then we can write $qa+xb=1$ so $qay+xby=y$ and therefore q divides y. If d is not a unit, then $q=du$ and $x=dv$ and since q is irreducible and d is not a unit, u must be a unit. Then d and q are associated and therefore q divides x.

Definition: A unique factorization domain (UFD) is an integral domain such that every nonzero element $r \in R$ which is not a unit is a product

$$r = p_1 p_2 \cdots p_n$$

where the p_i are (not necessarily distinct) irreducible elements of R and, if $r = q_1 q_2 \cdots q_k$ is another such factorization, then there is a rearrangement of the q_i so that q_i and p_i are associates.

Lemma: in a UFD, p is prime if and only if it is irreducible.

– This follows from uniquess of the factorization.

Lemma: A UFD has greatest common divisors (computed using the factorization into primes as in $\mathbb{Z}$).

There are two features of the UFD property. One is that every nonzero element is a finite product of irreducibles; and the other is that this is unique.

Theorem: A principal ideal domain is a UFD.

- Every element of a PID R that is not a unit is a finite product of irreducible elements.

Proof: Choose a non-unit x in R. Suppose x *does not* have a finite factorization into irreducibles. Write $x = a_1 b_1$ where a_1 and b_1 are non-units. Then one of a_1 or b_1 does not have a finite factorization into irreducibles; suppose it's a_1. Notice that $xR \subset a_1 R$ and the inclusion is strict since b is a non-unit. Repeat this argument to construct an increasing sequence of *proper* ideals

$$xR \subset a_1 R \subset a_2 R \subset \cdots$$

Let I be the union of all of these ideals inside R. This ideal must be principal, so $I = yR$ for some y. Now $y \in a_j R$ for some j, which means that at some point the increasing sequence stabilizes; $a_k R = yR$ for all $k \geq j$. This contradicts the assumption that x did not have a finite factorization.

For the uniqueness, we know that every element of R is a finite product of irreducible elements, and that irreducible elements in R are prime. We proceed by induction on n, the minimal number of irreducible elements needed to write x as a product. Suppose $n = 1$. Then x is irreducible and hence prime. Suppose that whenever x is a product of up to n irreducibles, that expression is unique. Suppose y is a product of $n + 1$ irreducibles and it has two factorizations

$$y = p_1 p_2 \cdots p_{n+1} = q_1 q_2 \cdots q_s$$

where $s \geq n + 1$. Since p_1 divides the product of the $q's$, it must equal one of the $q's$ up to a unit, so we can cancel p_1 from both sides of the equation. Now y/p_1 has a shorter expression as a product of irreducibles, so it's expression is unique, and therefore $s = n + 1$ and the $q's$ are a rearrangement of the $p's$.