MATH 171 FALL 2008: LECTURE 15

DAGAN KARP

1. Euclidean Domains

Throughout this lecture, all rings are assumed commutative.

The goal of this lecture is to introduce and discuss Euclidean Domains. We already have experience with domains, i.e. rings without zero divisors, so the new ingredient here is the adjective Euclidean. There are two requirements for a domain to be considered Euclidean. First, as with Euclidean metric spaces, the domain must have a notion of "measure" or "norm."

Definition 1. *A* norm N *on the integral domain* R *is a map of sets*

$$N : R \to \mathbb{N} \cup \{0\}$$

such that $N(0) = 0$.

Further, if $N(a) > 0$ *for all* $a \neq 0$*, then we say* N *is a* positive norm*.*

Remark 2. This is a pretty lame definition of norm, but some people use it, including Dummit and Foote, so for consistency we'll use it as well. But it's worth noting that this is a really weak definition, in that any such map of sets qualifies. If we required that N satisfied a triangle inequality $N(a + b) \leqslant N(a) + N(b)$ or $N(ab) \leqslant N(a)N(b)$, it would feel much more like a norm to me. But, alas, we'll make no such requirement.

In addition to the requirement of norm, a Euclidean domain has a good notion of divisibility.

Definition 3. *The integral domain* R *is called a* Euclidean domain *if there is a norm* N *on* R *such that if* $a, b \in R$ *and* $b \neq 0$*, then there exists elements* $q, r \in R$ *such that*

$$a = qb + r,$$

where $r = 0$ *or* $N(r) < N(b)$*. The element* q *is called the quotient and* r *the remainder.*

This feels very much like ordinary division of integers, and indeed is a direct generalization.

Example 4. *The integers* $\mathbb{Z}$ *are a Euclidean domain with* $N(a) = |a|$*. First, note that* $|\cdot|$ *is indeed a map of sets* $\mathbb{Z} \to \mathbb{N} \cup \{0\}$ *and that* $|0| = 0$*.*

Now we need to know that division works in $\mathbb{Z}$*. For sport, let's prove this directly.*

Date: October 27, 2008.

Claim. For any $a, b \in \mathbb{Z}$ *with* $b > 0$*, there exist unique* $q, r \in \mathbb{Z}$ *such that*

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

Proof. (Existence) If $a \geqslant 0$*, we proceed by induction. First, suppose* $a < b$*. Then choosing* $q = 0$ *and* $r = a$*, we are done.*

Now suppose $a \geqslant b$*. To induce, we also suppose that our claim is satisfied and*

$$a = qb + r.$$

We must inspect $a + 1$*. But*

$$a + 1 = qb + r + 1.$$

So, if $r + 1 < b$*, then we our proof is complete. But* $r < b$ *by hypothesis, so* $r + 1 \leqslant b$*. The remaining possibility is thus* $r + 1 = b$*. In that case*

$$a + 1 = qb + r + 1 = qb + b = b(q + 1),$$

and our quotient is $q + 1$ *and remainder* 0*. Hence the proof holds in case* $a \geqslant 0$*.*

Now suppose $a < 0$*. Then* $-a > 0$ *and by the above, there exist* q, r *such that* $-a = qb + r$ *and* $0 \leqslant r < b$*. If* $r = 0$*, then*

$$a = b(-q) + 0$$

and the claim holds. Otherwise $r > 0$*, and*

$$a = b(-q) - r = b(-q - 1) + (b - r),$$

and the claim holds with quotient $-q - 1$ *and remainder* $0 \leqslant b - r < b$*.*

(Uniqueness) Assume that $a = qb + r = q'b + r'$ *with* $0 \leqslant r, r' < b$*. Then*

$$-b < r - r' < b.$$

Also, this difference

$$r - r' = b(q - q')$$

is a multiple of b*. Any nonzero integer multiple of* b *is either greater than or equal to* b *or less than or equal to* $-b$*. Therefore* $r - r'$ *must be zero. Hence also* $qb = q'b$ *and so* $q = q'$*.* □

As with the integers, there is an algorithm for division in Euclidean domains.

Definition 5. *The* Euclidean algorithm *for two elements* a, b *in an integral domain* R *is a list of divisions*

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n, \end{aligned}$$

where r_n *is the last nonzero remainder. Such an* r_n *exists, as*

$$N(r_1) > N(r_2) > \cdots > N(r_n) \geqslant 0$$

is a decreasing sequence of non-negative integers.

Example 6. *If* F *is a field, then* $F[x]$ *is a Euclidean domain with*

$$N(f(x)) = \deg(f(x)).$$

The Euclidean algorithm here is the familiar polynomial long division. For instance, let $f, g \in \mathbb{Z}_5[x]$ *be given by* $f = 3x^4 + x^3 + 2x^2 + 1$ *and* $g = x^2 + 4x + 2$*. Then*

$$\begin{array}{r}
3x^2+4x \\
x^2+4x+2\sqrt{3x^4+x^3+2x^2+1} \\
\underline{3x^4+2x^3+x^2} \\
4x^3+x^2+1 \\
\underline{4x^3+x^2+3x} \\
2x+1
\end{array}$$

Note that we could have obtained the same result using polynomial long division in $\mathbb{Z}$*, and then reduced our answer modulo* 5*.*

$$\begin{array}{rrrrrr}
 & & & 3x^2 & -11x & +40 \\ \cline{2-6}
x^2+4x+2\big) & 3x^4 & +x^3 & +2x^2 & & +1 \\
 & -3x^4 & -12x^3 & -6x^2 & & \\ \cline{2-4}
 & & -11x^3 & -4x^2 & & \\
 & & 11x^3 & +44x^2 & +22x & \\ \cline{3-5}
 & & & 40x^2 & +22x & +1 \\
 & & & -40x^2 & -160x & -80 \\ \cline{4-6}
 & & & & -138x & -79
\end{array}$$

Example 7. *The ring of Gaussian integers*

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

is a Euclidean domain with norm

$$N(a + bi) = a^2 + b^2.$$

Definition 8. *Let* $a, b \in R$ *be elements of the ring* R *with* $b \neq 0$*. Then* a is a multiple of b *if there is an element* $q \in R$ *such that* $a = bq$*. Then we also say* b divides a*, or*b is a divisor of a*, denoted* $b|a$*.*

Definition 9. *The* greatest common divisor *of* a *and* b *is a nonzero element* $d \in R$ *such that*

(1) $d|a$ *and* $d|b$
(2) *if* $c|a$ *and* $c|b$*, then* $c|d$*.*

The greatest common divisor is denoted $d = \gcd(a, b)$ *or simply* $d = (a, b)$*.*

Proposition 10. *If* a *and* b *are nonzero elements in the commutative ring* R *such that the ideal generated by* a *and* b *is principal,* $(a, b) = (d)$*, then* $d = \gcd(a, b)$.

Remark 11. An integral domain such that every ideal generated by two elements is principal is called a *Bezout domain.*

Proposition 12. *Let* R *be an integral domain. Let* $d, d' \in R$*. If* $(d) = (d')$*, then there exists a unit* $u \in R$ *such that* $d' = ud$.

Proof. If $d = 0$ we are done. Otherwise, we have $d = xd'$ and $d' = yd$. Thus $d = xyd$, and hence $d(1 - xy) = 0$. Thus $xy = 1$ and both x and y are units. □

Theorem 13. *Let* R *be a Euclidean domain and let* $0 \neq a, b \in R$*. Let* $d = r_n$ *be the last nonzero remainder in the Euclidean algorithm of* a *and* b*. Then*

(1) $d = \gcd(a, b)$
(2) $d = (a, b)$.

Remark 14. Note that (2) above implies there exist elements $x, y \in R$ such that

$$d = ax + by.$$

Theorem 15. *Suppose that* $ax_0 + by_0 = c$*. Then all solutions* x, y *of the equation* $ax + by = c$ *are of the form*

$$x = x_0 + m\frac{b}{(a, b)}$$
$$y = y_0 - m\frac{a}{(a, b)},$$

for some integer m.

Proof. Dummit and Foote, problem (8.1) # 4.

Remark 16. Note that the equation

$$ax + by = c$$

has integer solutions $x, y \in \mathbb{Z}$ if and only if c is in the ideal generated by a and b. But this ideal is generated by the greatest common divisor $(a, b) = (d)$. Thus the equation is solvable if and only if $c \in (d)$, i.e. c is a multiple of d. To repeat, an integral solution to this equation exists if and only if c is divisible by the greatest common divisor of a and b. In that case, all solutions are given by the above theorem.

Example 17. *The equation*

$$3x + 12y = 17$$

has no solutions, as 17 *is prime, but* $(3, 12) = 3$*. In particular,* 17 *is not a multiple of* 3.