$\widetilde{R} = R^{\times} \cup \{0\}$ denote the collection of units of R together with 0. An element $u \in R - \widetilde{R}$ is called a *universal side divisor* if for every $x \in R$ there is some $z \in \widetilde{R}$ such that u divides $x - z$ in R, i.e., there is a type of "division algorithm" for u: every x may be written $x = qu + z$ where z is either zero or a unit. The existence of universal side divisors is a weakening of the Euclidean condition:

Proposition 5. Let R be an integral domain that is not a field. If R is a Euclidean Domain then there are universal side divisors in R.

Proof: Suppose R is Euclidean with respect to some norm N and let u be an element of $R - \widetilde{R}$ (which is nonempty since R is not a field) of minimal norm. For any $x \in R$, write $x = qu + r$ where r is either 0 or $N(r) < N(u)$. In either case the minimality of u implies $r \in \widetilde{R}$. Hence u is a universal side divisor in R.

Example

We can use Proposition 5 to prove that the quadratic integer ring $R = \mathbb{Z}[(1+\sqrt{-19})/2]$ is not a Euclidean Domain with respect to any norm by showing that R contains no universal side divisors (we shall see in the next section that all of the ideals in R are principal, so the technique in the examples following Proposition 1 do not apply to this ring). We have already determined that ± 1 are the only units in R and so $\widetilde{R} = \{0, \pm 1\}$. Suppose $u \in R$ is a universal side divisor and let $N(a + b(1 + \sqrt{-19})/2) = a^2 + ab + 5b^2$ denote the field norm on R as in Section 7.1. Note that if $a, b \in \mathbb{Z}$ and $b \neq 0$ then $a^2 + ab + 5b^2 = (a + b/2)^2 + 19/4b^2 \geq 5$ and so the smallest nonzero values of N on R are 1 (for the units ± 1) and 4 (for ± 2). Taking $x = 2$ in the definition of a universal side divisor it follows that u must divide one of $2 - 0$ or 2 ± 1 in R, i.e., u is a nonunit divisor of 2 or 3 in R. If $2 = \alpha\beta$ then $4 = N(\alpha)N(\beta)$ and by the remark above it follows that one of α or β has norm 1, i.e., equals ± 1. Hence the only divisors of 2 in R are $\{\pm 1, \pm 2\}$. Similarly, the only divisors of 3 in R are $\{\pm 1, \pm 3\}$, so the only possible values for u are ± 2 or ± 3. Taking $x = (1 + \sqrt{-19})/2$ it is easy to check that none of $x, x \pm 1$ are divisible by ± 2 or ± 3 in R, so none of these is a universal side divisor.

EXERCISES

1. For each of the following five pairs of integers a and b, determine their greatest common divisor d and write d as a linear combination $ax + by$ of a and b.
   (a) $a = 20, b = 13$.
   (b) $a = 69, b = 372$.
   (c) $a = 11391, b = 5673$.
   (d) $a = 507885, b = 60808$.
   (e) $a = 91442056588823$, $b = 779086434385541$ (the Euclidean Algorithm requires only 7 steps for these integers).
2. For each of the following pairs of integers a and n, show that a is relatively prime to n and determine the inverse of a mod n (cf. Section 3 of the Preliminaries chapter).
   (a) $a = 13, n = 20$.
   (b) $a = 69, n = 89$.
   (c) $a = 1891, n = 3797$.

(d) $a = 6003722857, n = 77695236973$ (the Euclidean Algorithm requires only 3 steps for these integers).

3. Let R be a Euclidean Domain. Let m be the minimum integer in the set of norms of nonzero elements of R. Prove that every nonzero element of R of norm m is a unit. Deduce that a nonzero element of norm zero (if such an element exists) is a unit.

4. Let R be a Euclidean Domain.

   (a) Prove that if $(a, b) = 1$ and a divides bc, then a divides c. More generally, show that if a divides bc with nonzero a, b then $\dfrac{a}{(a,b)}$ divides c.

   (b) Consider the Diophantine Equation $ax + by = N$ where a, b and N are integers and a, b are nonzero. Suppose x_0, y_0 is a solution: $ax_0 + by_0 = N$. Prove that the full set of solutions to this equation is given by

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

   as m ranges over the integers. [If x, y is a solution to $ax + by = N$, show that $a(x - x_0) = b(y_0 - y)$ and use (a).]

5. Determine all integer solutions of the following equations:

   (a) $2x + 4y = 5$

   (b) $17x + 29y = 31$

   (c) $85x + 145y = 505$.

6. (*The Postage Stamp Problem*) Let a and b be two relatively prime positive integers. Prove that every sufficiently large positive integer N can be written as a linear combination $ax + by$ of a and b where x and y are both *nonnegative*, i.e., there is an integer N_0 such that for all $N \geq N_0$ the equation $ax + by = N$ can be solved with both x and y nonnegative integers. Prove in fact that the integer $ab - a - b$ cannot be written as a positive linear combination of a and b but that every integer greater than $ab - a - b$ is a positive linear combination of a and b (so every "postage" greater than $ab - a - b$ can be obtained using only stamps in denominations a and b).

7. Find a generator for the ideal $(85, 1+13i)$ in $\mathbb{Z}[i]$, i.e., a greatest common divisor for 85 and $1+13i$, by the Euclidean Algorithm. Do the same for the ideal $(47 - 13i, 53 + 56i)$.

It is known (but not so easy to prove) that $D = -1, -2, -3, -7, -11, -19, -43, -67$, and -163 are the only negative values of D for which every ideal in $\mathcal{O}$ is principal (i.e., $\mathcal{O}$ is a P.I.D. in the terminology of the next section). The results of the next exercise determine precisely which quadratic integer rings with $D < 0$ are Euclidean.

8. Let $F = \mathbb{Q}(\sqrt{D})$ be a quadratic field with associated quadratic integer ring $\mathcal{O}$ and field norm N as in Section 7.1.

   (a) Suppose D is $-1, -2, -3, -7$ or -11. Prove that $\mathcal{O}$ is a Euclidean Domain with respect to N. [Modify the proof for $\mathbb{Z}[i]$ ($D = -1$) in the text. For $D = -3, -7, -11$ prove that every element of F differs from an element in $\mathcal{O}$ by an element whose norm is at most $(1 + |D|)^2/(16|D|)$, which is less than 1 for these values of D. Plotting the points of $\mathcal{O}$ in $\mathbb{C}$ may be helpful.]

   (b) Suppose that $D = -43, -67$, or -163. Prove that $\mathcal{O}$ is not a Euclidean Domain with respect to any norm. [Apply the same proof as for $D = -19$ in the text.]

9. Prove that the ring of integers $\mathcal{O}$ in the quadratic integer ring $\mathbb{Q}(\sqrt{2})$ is a Euclidean Domain with respect to the norm given by the absolute value of the field norm N in Section 7.1.

10. Prove that the quotient ring $\mathbb{Z}[i]/I$ is finite for any nonzero ideal I of $\mathbb{Z}[i]$. [Use the fact

that $I = (\alpha)$ for some nonzero α and then use the Division Algorithm in this Euclidean Domain to see that every coset of I is represented by an element of norm less than $N(\alpha)$.]

11. Let R be a commutative ring with 1 and let a and b be nonzero elements of R. A *least common multiple* of a and b is an element e of R such that
   (i) $a \mid e$ and $b \mid e$, and
   (ii) if $a \mid e'$ and $b \mid e'$ then $e \mid e'$.

(a) Prove that a least common multiple of a and b (if such exists) is a generator for the unique largest principal ideal contained in $(a) \cap (b)$.

(b) Deduce that any two nonzero elements in a Euclidean Domain have a least common multiple which is unique up to multiplication by a unit.

(c) Prove that in a Euclidean Domain the least common multiple of a and b is $\dfrac{ab}{(a, b)}$, where (a, b) is the greatest common divisor of a and b.

12. (*A Public Key Code*) Let N be a positive integer. Let M be an integer relatively prime to N and let d be an integer relatively prime to $\varphi(N)$, where φ denotes Euler's φ-function. Prove that if $M_1 \equiv M^d \pmod N$ then $M \equiv M_1^{d'} \pmod N$ where d' is the inverse of d mod $\varphi(N)$: $dd' \equiv 1 \pmod{\varphi(N)}$.

Remark: This result is the basis for a standard *Public Key Code*. Suppose $N = pq$ is the product of two distinct large primes (each on the order of 100 digits, for example). If M is a message, then $M_1 \equiv M^d \pmod N$ is a scrambled (*encoded*) version of M, which can be unscrambled (*decoded*) by computing $M_1^{d'} \pmod N$ (these powers can be computed quite easily even for large values of M and N by successive squarings). The values of N and d (but not p and q) are made publicly known (hence the name) and then anyone with a message M can send their encoded message $M^d \pmod N$. To decode the message it seems necessary to determine d', which requires the determination of the value $\varphi(N) = \varphi(pq) = (p-1)(q-1)$ (no one has as yet *proved* that there is no other decoding scheme, however). The success of this method as a code rests on the necessity of determining the *factorization* of N into primes, for which no sufficiently efficient algorithm exists (for example, the most naive method of checking all factors up to $\sqrt{N}$ would here require on the order of 10^{100} computations, or approximately 300 years even at 10 billion computations per second, and of course one can always increase the size of p and q).

8.2 PRINCIPAL IDEAL DOMAINS (P.I.D.s)

Definition. A *Principal Ideal Domain* (P.I.D.) is an integral domain in which every ideal is principal.

Proposition 1 proved that *every Euclidean Domain is a Principal Ideal Domain* so that every result about Principal Ideal Domains automatically holds for Euclidean Domains.

Examples

(1) As mentioned after Proposition 1, the integers $\mathbb{Z}$ are a P.I.D. We saw in Section 7.4 that the polynomial ring $\mathbb{Z}[x]$ contains nonprincipal ideals, hence is not a P.I.D.

(2) Example 2 following Proposition 1 showed that the quadratic integer ring $\mathbb{Z}[\sqrt{-5}\,]$ is not a P.I.D., in fact the ideal $(3, 1 + \sqrt{-5}\,)$ is a nonprincipal ideal. It is possible