

**Mathematics 361: Number Theory**  
**Assignment #1**

**Reading:** Ireland and Rosen, Chapter 1 (including the exercises)

**Problems:**

Euclidean algorithm and linear Diophantine equations:

1. Let  $0 < b < a$ . The Euclidean algorithm is:

- (Initialize) Set  $r_{-1} = a$ ,  $r_0 = b$ ,  $j = 1$ .
- (Carry out the  $j^{\text{th}}$  divide) Define  $q_j$  and  $r_j$  by the conditions

$$r_{j-2} = q_j r_{j-1} + r_j, \quad r_j < r_{j-1}.$$

If  $r_j = 0$ , go to the next step; otherwise increment  $j$  and repeat this step.

- (Output) Return running time  $n = j$  and  $\gcd(a, b) = r_{n-1}$ .

Thus the net effect is

$$\begin{aligned} a &= q_1 b + r_1, & 0 < r_1 < b \\ b &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2 \\ &\vdots \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\ r_{n-2} &= q_n r_{n-1}. \end{aligned}$$

(a) Explain why the algorithm must terminate. Give a crude upper bound for the running time.

(b) Show that the quantities in Step (2) obey the relation  $(r_j, r_{j-1}) = (r_{j-1}, r_{j-2})$  (the parentheses can denote greatest common divisors or ideals, whichever you prefer). How does this justify the claim that at the end of the algorithm  $r_{n-1} = \gcd(a, b)$ ?

(c) Show that for some  $A$  and  $B$ ,  $Ar_{n-2} + Br_{n-1} = \gcd(a, b)$ . In Step (2), show that if for some  $A$  and  $B$ ,  $Ar_{j-1} + Br_j = \gcd(a, b)$ , then also for some  $A'$  and  $B'$ ,  $A'r_{j-2} + B'r_{j-1} = \gcd(a, b)$ . Thus for some  $A$  and  $B$ ,  $Aa + Bb = \gcd(a, b)$ .

(d) Work Ireland and Rosen, Exercises 1.3, 1.5—1.8, 1.13, 1.14.

Some ring theory:

2. (a) Let  $R$  be a commutative ring with 1. Show that  $R$  is an integral domain if and only if the cancellation law holds.

(b) Show that if  $R$  is a field then  $R$  is an integral domain.

3. Prove that  $\mathbf{Q}(i) = \mathbf{Q}[i]$  and  $\mathbf{Q}(\omega) = \mathbf{Q}[\omega]$ .

4. Consider the ring  $R = \mathbf{Z}[\sqrt{-5}]$ . Show that the ideal  $(2, 1 + \sqrt{-5})$  is not principal, so  $R$  is not a PID. Use the norm  $N(x + y\sqrt{-5}) = x^2 + 5y^2$  to show that 2 is irreducible in  $R$  but not prime in  $R$  since  $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ .

Mersenne primes and Fermat primes, cf. Ireland and Rosen, Exercises 1.24—1.26:

5. Let  $a \geq 2$  and  $n \geq 2$ . Use the geometric sum formula and its variant

$$r^n - 1 = (r - 1) \sum_{j=0}^{n-1} r^j, \quad r^n + 1 = (r + 1) \sum_{j=0}^{n-1} (-1)^j r^j \quad \text{for } n \text{ odd}$$

to prove that (a) if  $a^n - 1$  is prime then  $a = 2$  and  $n$  is prime (such  $2^p - 1$  primes are called *Mersenne primes*); (b) if  $a^n + 1$  is prime then  $a$  is even and  $n$  is a power of 2 (in particular,  $2^{2^n} + 1$  primes are called *Fermat primes*).

Incidentally, the geometric sum formula and its variant quickly yield the identities

$$x^n - y^n = (x - y) \sum_{j=0}^{n-1} x^{n-1-j} y^j$$

and

$$x^n + y^n = (x + y) \sum_{j=0}^{n-1} (-1)^j x^{n-1-j} y^j \quad \text{for } n \text{ odd,}$$

which should be familiar from high school for small values of  $n$ .

No polynomial generates a sequence of prime values:

6. Let  $f$  be a nonconstant polynomial with integer coefficients.

(a) If  $f$  has degree  $n$  show that

$$f(x + h) = f(x) + \frac{f'(x)}{1!} h + \frac{f''(x)}{2!} h^2 + \cdots + \frac{f^{(n)}(x)}{n!} h^n.$$

(One can show this using Taylor's Theorem with Remainder or prove it as a formal polynomial identity.) Note that each  $f^{(j)}(x)/j!$  also has integer coefficients.

(b) Show that the sequence

$$\{f(1), f(2), f(3), \dots\}$$

does not consist solely of primes past any starting index, as follows. Without loss of generality, the leading coefficient of  $f$  is positive, so  $f(n_0) > 1$  for some integer  $n_0$  beyond which  $f$  is monotone increasing; then  $f(n_0 + kf(n_0))$  is composite for all  $k \geq 1$ .

(The polynomial expression  $x^2 - x + 41$  is prime for  $0 \leq x \leq 40$ .)