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 \([x, y; \alpha, \beta, \gamma, \delta; s] = [a, b; 1, 0, 0, 1; 0]\).
   - (Divide) We have \( x = qy + r, 0 \leq r < y \); set
     \([x, y; \alpha, \beta, \gamma, \delta; s] = [y, r; \gamma, \delta, \alpha - q\gamma, \beta - q\delta; s + 1]\).
     If \( y = 0 \), go to the next step; otherwise repeat this step.
   - (Output) Return \( x; \alpha, \beta; s \). Here \( x = \gcd(a, b) = \alpha a + \beta b \), and the running time is \( s \).

(a) Show that after the initialization step,
\[ (x, y) = (a, b), \quad x = \alpha a + \beta b, \quad y = \gamma a + \delta b. \]

(b) Show that each division step preserves the conditions by showing that
\[ (x_{\text{new}}, y_{\text{new}}) = (a, b), \]
\[ x_{\text{new}} = \alpha_{\text{new}} a + \beta_{\text{new}} b, \]
\[ y_{\text{new}} = \gamma_{\text{new}} a + \delta_{\text{new}} b, \]
given that these relations are established with “old” instead of “new” throughout.

(c) Show that at termination the conditions are
\[ (x) = (a, b), \]
\[ x = \alpha a + \beta b. \]

Thus \( x = \gcd(a, b) \) (the positive greatest common divisor), and we have expressed \( \gcd(a, b) \) as a linear combination of \( a \) and \( b \).

(d) The algorithm generates a succession of remainders
\[ r_{-1} = a, \]
\[ r_0 = b, \]
\[ r_k = r_{k-2} - q_k r_{k-1}, \quad k = 1, \cdots, s, \]
with each \( q_k \geq 1 \) and
\[
    r_{-1} > r_0 > r_1 > \cdots > r_{s-1} > r_s = 0, \quad s \geq 1.
\]
Here \( s \) is the number of steps that the algorithm takes. Let \( F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, \) and so on be the Fibonacci numbers. Thus we have
\[
    r_{s-1} \geq 1 = F_2, \\
    r_{s-2} \geq 2 = F_3, \\
    r_{s-3} \geq r_{s-2} + r_{s-1} \geq F_4, \\
    \vdots \\
    b = r_0 = r_{s-s} \geq F_{s+1}.
\]
A lemma (see page 72 of Jamie Pommersheim’s book) that you may take for granted or prove says that \( F_{k+2} > \varphi^k \) for \( k \geq 1 \), where \( \varphi \) is the Golden Ratio. Show that consequently an integer upper bound on the number \( s \) of steps for the Euclidean algorithm to compute \( \gcd(a, b) \) where \( 0 < b < a \) is
\[
    \lceil \log_\varphi(b) \rceil \geq s.
\]
(e) Work Ireland and Rosen, Exercises 1.3, 1.5—1.8, 1.13, 1.14. For 1.13, let \( g \) be the generator of the ideal generated by the \( n_i \) and argue that \( g \) is the gcd of the \( n_i \). Then use this idea in 1.14. Also, 1.6 can be done tidily by using ideals.

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 \( \mathbb{Q}(i) = \mathbb{Q}[i] \) and \( \mathbb{Q}(\omega) = \mathbb{Q}[\omega] \).
4. Consider the ring \( R = \mathbb{Z}[(\sqrt{-5})]. \) 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

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

for $n$ 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

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

for $n$ 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

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

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 $0 \leq x \leq 40$.)