Mathematics 361: Number Theory
Assignment A

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

Problems:

The Euclidean algorithm.
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 $x = qy + r$, $0 \le r < y$; 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 bullet; otherwise repeat this one.
- (Output) Return x; α, β; s. Here $x = \gcd(a, b) = \alpha a + \beta b$, and the running time is s. (Here s stands for *steps.*)

For example, to compute $\gcd(986, 357)$ the algorithm proceeds as follows:

x	y	α	β	γ	δ	s	calculation for next line
986	357	1	0	0	1	0	$986 = 2 \cdot 357 + 272$
357	272	0	1	1	-2	1	$357 = 1 \cdot 272 + 85$
272	85	1	-2	-1	3	2	$272 = 3 \cdot 85 + 17$
85	17	-1	3	4	-11	3	$85 = 5 \cdot 17$
17	0	4	-11			4	

Thus $\gcd(986, 357) = 17 = 4 \cdot 986 - 11 \cdot 357$, and the algorithm took 4 steps.

The questions to follow are about the general case of the algorithm, not the particular example just given.

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

(b) Show that each division preserves the conditions by showing that
$$\begin{aligned} (x_{\text{new}}, y_{\text{new}}) &= (a, b), \\ x_{\text{new}} &= \alpha_{\text{new}} a + \beta_{\text{new}} b, \\ y_{\text{new}} &= \gamma_{\text{new}} a + \delta_{\text{new}} b, \end{aligned}$$
given that these relations are established with "old" instead of "new" throughout.

(c) Show that at termination the conditions are

$$\begin{aligned}(x) &= (a, b),\\ x &= \alpha a + \beta b.\end{aligned}$$

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

$$\begin{aligned}r_{-1} &= a,\\ r_0 &= b,\\ r_k &= r_{k-2} - q_k r_{k-1}, \quad k = 1, \cdots, s,\end{aligned}$$

with each $q_k \geq 1$ and

$$r_{-1} > r_0 > r_1 > \cdots > r_{s-1} > r_s = 0, \quad s \geq 1.$$

Again, 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

$$\begin{aligned}r_{s-1} &\geq 1 = F_2,\\ r_{s-2} &\geq 2 = F_3,\\ r_{s-3} &\geq r_{s-2} + r_{s-1} \geq F_4,\\ &\vdots\\ b = r_0 = r_{s-s} &\geq F_{s+1}.\end{aligned}$$

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 $\varphi = (1+\sqrt{5})/2$ is the Golden Ratio. Show that consequently, if the Euclidean algorithm to compute $\gcd(a, b)$ where $0 < b < a$ requires $s \geq 2$ steps then an integer upper bound of the step-count is

$$\boxed{\lceil \log_\varphi(b) \rceil \geq s.}$$

So long as b is greater than 1, this formula covers the case $s = 1$ as well. Even though running the Euclidean algorithm with $b = 1$ is silly, we could well instruct a computer to do so by omitting to code a special-case check. Changing the left side of the boxed formula to the maximum of $\lceil \log_\varphi(b) \rceil$ and 1 covers all cases.

(e) Work Ireland and Rosen exercises 1.3 (just the first part, but do it demonstrating the method at the beginning of this exercise), 1.6–1.8, 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.

2. Prove that $\mathbb{Z}(i) \subset \mathbb{Q}[i]$. Obviously $\mathbb{Q}[i] \subset \mathbb{Q}(i)$. Prove that $\mathbb{Q}(i) \subset \mathbb{Z}(i)$, and so all three are equal. The same can be done with ω in place of i, but there is no need because we will do this in fuller generality later. The point of this exercise is that Ireland and Rosen in chapter 1 tacitly use the relations $\mathbb{Z}(i) = \mathbb{Q}[i]$ and $\mathbb{Z}(\omega) = \mathbb{Q}[\omega]$ in proving that $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ with the usual norm $\mathrm{N}z = z\overline{z}$ are Euclidean.

3. (a) Show that for any squarefree negative integer $n \equiv 2, 3 \pmod 4$, the ring $R = \mathbb{Z}[\sqrt{n}]$ is only the lattice $\mathbb{Z} \oplus \mathbb{Z}\sqrt{n}$. For what such n is this ring with the usual norm Euclidean?

(b) Show that for any squarefree negative integer $n \equiv 1 \pmod 4$, the ring $R = \mathbb{Z}[(1+\sqrt{n})/2]$ is only the lattice $\mathbb{Z} \oplus \mathbb{Z}(1+\sqrt{n})/2$. For what such n is this ring with the usual norm Euclidean?

Mersenne primes and Fermat primes; cf. Ireland and Rosen exercises 1.24–1.26.

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

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

and

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

to prove that (a) if $a^n - 1$ is prime (now safely using *prime* as a synonym for *irreducible* when talking about positive integers) 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.

5. 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 $0 \leq x \leq 40$. You are not being asked to show this.)