

Mathematics 361: Number Theory
Assignment #2

Reading: Ireland and Rosen, Chapter 2 (including the exercises)

Problems:

Upper bound for Euclidean algorithm efficiency:

1. Let $0 < b < a$, a not divisible by b , and suppose the Euclidean algorithm requires n steps to determine $\gcd(a, b)$. In other words, $\gcd(a, b) = r_{n-1}$ where

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

Thus if we define $r_{-1} = a$, $r_0 = b$, $r_n = 0$, the general step is

$$r_{j-2} = q_j r_{j-1} + r_j, \quad r_j < r_{j-1} \quad (1 \leq j \leq n)$$

or

$$r_j = q_{j+2} r_{j+1} + r_{j+2}, \quad r_{j+2} < r_{j+1} \quad (-1 \leq j \leq n-2).$$

(a) Show: $q_j \geq 1$ for $1 \leq j \leq n$, so $r_j \geq r_{j+1} + r_{j+2}$ for $-1 \leq j \leq n-2$.

(b) Show: $r_{n-k} \geq u_k$ for $1 \leq k \leq n$ where $u_0 = u_1 = 1$ and $u_k = u_{k-1} + u_{k-2}$ for $k \geq 2$. (The u_k are the *Fibonacci numbers*.) In particular, $b \geq u_n$.

(c) Show: If $\tau = (1 + \sqrt{5})/2$ then $\tau^2 = \tau + 1$ and more generally $\tau^j = u_{j-1}\tau + u_{j-2}$ for $j \geq 2$. (The number τ is the *Golden Ratio*.) Show that $b > \tau^{n-1}$.

(d) Show: If b has d base 10 digits then $n \leq 5d$. Thus the number of divisions in the Euclidean algorithm never exceeds five times the number of base 10 digits of the smaller of the two numbers. (Note $b < 10^d$ and $\log_{10} \tau = 0.2 \dots$.) Does your experience suggest that this is a tight bound?

Even perfect numbers (nobody knows if there are any odd ones):

2. (a) Show that if $2^p - 1$ is prime (forcing p to be prime) then $2^{p-1}(2^p - 1)$ is perfect.

(b) If m is even and perfect, show that m takes the form $m = 2^{p-1}(2^p - 1)$ where $2^p - 1$ is prime. (Write $m = 2^{p-1}t$ where $p \geq 2$ and t is odd and we don't yet know whether p is prime. Show that $t \neq 1$. Show that $\sigma(t) = 2^p r$ where r is odd and $t = (2^p - 1)r$. Show that $r = 1$ and $2^p - 1$ is prime.)

(c) Where does the argument in (b) break down if $p = 1$? That is, why can't we argue as in (b) to show that there are no odd perfect numbers?

3. Work Ireland and Rosen, Exercises 1.30, some of 1.32—1.38.

More ring theory:

4. Let R be a commutative ring. Consider an increasing chain of ideals in R ,

$$I_0 \subset I_1 \subset I_2 \subset \cdots .$$

Let $I = \bigcup_{n \geq 0} I_n$. Show that I is an ideal in R .

5. In class we showed that if R is an integral domain in which every irreducible element is prime and for which the Noetherian property holds, then R is a UFD. Conversely, show that if R is a UFD then every irreducible element is prime and the Noetherian property holds for **principal** ideals. (Warning: there exist UFDs for which the Noetherian property fails.)