Week 2 Summary

Lecture 3

Suppose that r_0 and r_1 are nonnegative integers, not both zero. Choose the notation so that $r_0 \geq r_1$. The greatest common divisor $d = \gcd(r_0, r_1)$ can be found as follows.
If $r_1 = 0$ then the gcd is just r_0. (For example, $\gcd(6, 0) = 6$. Remember that 0 is a multiple of everything!) If $r_1 > 0$ then divide r_0 by r_1 to get a quotient a_1 and remainder r_2. If $r_2 = 0$ then the gcd is r_1; otherwise, divide r_2 into r_1, obtaining quotient a_2 and remainder r_3. Continue in this way until a remainder of zero is obtained. So we get the following setup, where the r_i's and a_i's are integers:

$$\begin{aligned} r_0 &= a_1 r_1 + r_2 \qquad (0 < r_2 < r_1) \\ r_1 &= a_2 r_2 + r_3 \qquad (0 < r_3 < r_2) \\ r_2 &= a_3 r_3 + r_4 \qquad (0 < r_4 < r_3) \\ &\vdots \\ r_{k-2} &= a_{k-1} r_{k-1} + r_k \qquad (0 < r_k < r_{k-1}) \\ r_{k-1} &= a_k r_k. \end{aligned}$$

Using the proposition from the end of Lecture 2 we see that

$$\gcd(r_0, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \cdots = \gcd(r_{k-1}, r_k) = \gcd(r_k, 0) = r_k.$$

That is, d (the gcd of r_0 and r_1) equals r_k, the last nonzero remainder obtained in the above process.
It is always possible to find integers p and q such that $pr_1 + qr_0 = \gcd(r_0, r_1)$. One way to do this is by working backwards through the above equations. The second to last equation gives $r_k = (-a_{k-1})r_{k-1} + r_{k-2}$, expressing r_k as a linear combination of r_{k-1} and r_{k-2}. The equation previous to that expresses r_{k-1} in terms of r_{k-2} and r_{k-3}, and if we substitute this expression for r_{k-1} into our expression for r_k we get r_k expressed in terms of r_{k-3} and r_{k-2}. But the next equation back gives a formula for r_{k-2}, and substituting this into the formula for r_k now expresses r_k in terms of r_{k-4} and r_{k-3}. Continuing like this we eventually get r_k expressed in terms of r_0 and r_1. See the example on pages 26, 27 of Walters' book.
There is way to do this, using something we call a *Magic Table*. Given a sequence of numbers a_1, a_2, a_3, ... , we define $p_{-1} = 0$, $p_0 = 1$ and $q_{-1} = 1$, $q_0 = 0$, and successively compute the numbers p_k and q_k in the following table

		a_1	a_2	a_3	a_4	$\cdots$
0	1	p_1	p_2	p_3	p_4	$\cdots$
1	0	q_1	q_2	q_3	q_4	$\cdots$

using the recurrence relations

$$\begin{aligned} p_k &= a_k p_{k-1} + p_{k-2} \\ q_k &= a_k q_{k-1} + q_{k-2} \end{aligned}$$

If one constructs this table using the sequence of quotients $a_1, a_2, \dots, a_k$ obtained in the Euclidean Algorithm calculation of $\gcd(r_0, r_1)$, then it turns out that the last pair of numbers p_k, q_k in the table are given by $p_k = r_0/d$ and $q_k = r_1/d$. The following proposition is easy to prove by induction.

***Proposition:** Let $a_1, a_2, a_3, \dots$ be any sequence of numbers, and for all integers $i \geq -1$ let p_i and q_i be the numbers in the Magic Table, as described above. Then for all positive integers n,

$$p_n q_{n+1} - p_{n+1} q_n = (-1)^n = \begin{cases} 1 & \text{if } n \text{ is even,} \\ -1 & \text{if } n \text{ is odd;} \end{cases}$$

and

$$p_n q_{n+2} - p_{n+2} q_n = (-1)^n a_{n+2}.$$

In particular, if $a_1, a_2, \dots, a_k$ are the quotients from the Euclidean Algorithm for $\gcd(r_0, r_1)$, then

$$p_{k-1}\frac{r_1}{d} - q_{k-1}\frac{r_0}{d} = p_{k-1}q_k - p_k q_{k-1} = (-1)^{k-1},$$

and so $(-1)^{k-1}p_{k-1}r_1 + (-1)^k q_{k-1} r_0 = d$. That is, the Magic Table gives us a way to find a pair of numbers p and q satisfying $pr_1 + qr_0 = \gcd(r_0, r_1)$: put $p = (-1)^{k-1}p_{k-1}$ and $q = (-1)^k q_{k-1}$.
Example: Does 288 have an inverse in $\mathbb{Z}_{377}$? If so, find it.
Applying the Euclidean Algorithm with $r_0 = 377$ and $r_1 = 288$ gives

$$\begin{aligned} 377 &= 1 \times 288 + 89 \\ 288 &= 3 \times 89 + 21 \\ 89 &= 4 \times 21 + 5 \\ 21 &= 4 \times 5 + 1 \\ 5 &= 5 \times 1 \end{aligned}$$

Thus the sequence of quotients a_i is 1, 3, 4, 4, 5. Now form the Magic Table.

		1	3	4	4	5
0	1	1	4	17	72	377
1	0	1	3	13	55	288

Now $72 \times 288 - 55 \times 377 = (-1)^4 = 1$. So $72 \times 288 \equiv 1 \pmod{377}$. So $72 = 288^{-1}$ in $\mathbb{Z}_{377}$.

***Proposition:** An element $a \in \mathbb{Z}_n$ has an inverse if and only if $\gcd(a, n) = 1$.

Lecture 4

Every real number can be uniquely expressed as the sum of its *integer part* and its *fractional part*, where here "fractional" means between 0 and 1 (including 0 but excluding 1).

Notation: $[x]$ = integer part of x = largest integer less than or equal to x.
The steps involved in the Euclidean Algorithm for $\gcd(248, 192)$ go as follows:

$$\begin{aligned} 248 &= 1 \times 192 + 56 \\ 192 &= 3 \times 56 + 24 \\ 56 &= 2 \times 24 + 8 \\ 24 &= 3 \times 8. \end{aligned}$$

We can rewrite these as follows:

$$\begin{aligned} \frac{248}{192} &= 1 + \frac{56}{192} \\ \frac{192}{56} &= 3 + \frac{24}{56} \\ \frac{56}{24} &= 2 + \frac{8}{24} \\ \frac{24}{8} &= 3. \end{aligned}$$

Putting these equations together gives

$$\frac{248}{192} = 1 + \frac{56}{192} = 1 + \frac{1}{192/56} = 1 + \frac{1}{3 + \frac{24}{56}} = \cdots$$

and eventually

$$\frac{248}{192} = 1 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{3}}} \quad .$$

Such expressions are called *continued fractions.*
We clearly need a more compact notation for continued fractions. Hence we make the following definition. If a_1, a_2, ... , a_k are any positive numbers, define

$$[a_1, a_2, \ldots, a_k] = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \; a_{k-1} + \cfrac{1}{a_k}}}} \quad .$$

If the a_i are positive integers then we call $[a_1, a_2, \ldots, a_k]$ a *simple continued fraction.* The numbers a_1, a_2, a_3, ... are called the *partial quotients*, and $[a_1]$, $[a_1, a_2]$, $[a_1, a_2, a_3]$, etc. the *convergents* of $[a_1, a_2, \ldots, a_k]$.
***Theorem:** If a_1, a_2, ..., a_k is any sequence of positive numbers, and for all i from -1 to k the numbers p_i, q_i are computed from the a_i's by means of a Magic Table, as above, then $[a_1, a_2, \ldots, a_k] = p_k/q_k$.
It is a fact that if p/q is a convergent of the continued fraction for a number α, then $|\alpha - (p/q)| < (1/q^2)$.