

Mathematics 361: Number Theory
Assignment #4

Reading: Ireland and Rosen, Chapter 4 (including the exercises)

Problems:

The pigeonhole principle and congruences:

1. Let m be a positive integer and a_1, \dots, a_m be any integers, possibly repeating. Show that for some nonempty subset S of the indices $\{1, \dots, m\}$, $\sum_{i \in S} a_i \equiv 0 \pmod{m}$. (Hint: pigeonhole the partial sums.)

The fifth Fermat number is composite:

2. Fermat defined the numbers $F_n = 2^{2^n} + 1$ for $n \geq 0$. Thus

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \\ F_4 = 65537, \quad F_5 = 4294967297, \quad \text{etc.}$$

He conjectured that all the F_n are prime, as indeed F_0 through F_4 are. Euler showed that F_5 is composite, using techniques that were actually available to Fermat and applied by him in similar situations. André Weil, in his book **Number Theory: An Approach Through History**, conjectures that Fermat tried these techniques on F_5 , made an arithmetic error (as he apparently often did), and never rechecked them. Following Euler, investigate whether F_5 is composite. To search for candidate prime factors p of F_5 , reason as follows: $p \mid 2^{32} + 1$ is equivalent to $2^{32} \equiv -1 \pmod{p}$, showing that 2 has order 64 in $(\mathbf{Z}/p\mathbf{Z})^*$. It follows that $64 \mid \phi(p) = p - 1$, so p must take the form $p = 64k + 1$. Thus candidates for p are

$$193, \quad 257, \quad 449, \quad 577, \quad 641, \quad \text{etc.}$$

Testing whether each of these primes p divides F_5 is easy. As above, we need to check whether $2^{32} \equiv -1 \pmod{p}$, so simply compute $2, 2^2, 2^4, 2^8$, etc. modulo p up to 2^{32} . Use this method to show that 193 does not divide F_5 . Neither do 257, 449 or 577, but don't bother showing this. Use this method to show that 641 *does* divide F_5 .

Note that this shows F_5 to be composite without ever computing it.

Using algebra rather than arithmetic:

3. The Fibonacci numbers are $u_0 = 0, u_1 = 1, u_n = u_{n-1} + u_{n-2}$ for $n \geq 2$ (this is slightly different indexing from earlier). Read through the following method to compute a closed form expression for u_n via linear algebra:

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. Induction quickly shows that $A^n = \begin{bmatrix} u_{n-1} & u_n \\ u_n & u_{n+1} \end{bmatrix}$ for $n \geq 1$. So to find u_n in closed form it suffices to compute either off-diagonal entry of A^n .

To diagonalize A with no mess, one easily computes that its characteristic polynomial is $\chi_A(\lambda) = \lambda^2 - \text{tr}(A)\lambda + \det(A) = \lambda^2 - \lambda - 1$. We let τ and τ' denote the roots of χ_A but we *don't compute them yet*—the numerical values only muddy the calculation. The coefficients of the characteristic polynomial show that

$$(1) \quad \tau + \tau' = 1, \quad \tau\tau' = -1.$$

Note that the second relation in (1) tells us that one root—say, τ —is positive and the other negative. Thus the roots are distinct and each corresponding eigenspace of A has dimension 1.

In particular, the matrix

$$A - \tau I = \begin{bmatrix} -\tau & 1 \\ 1 & 1 - \tau \end{bmatrix}$$

must have nullity 1 and therefore rank 1, meaning its two rows are linearly dependent so that any vector orthogonal to the first row spans the matrix's nullspace. For example, $\begin{bmatrix} 1 \\ \tau \end{bmatrix}$ works. Continuing this argument shows that

$$A^n = PJ^nP^{-1} \quad \text{where } J = \begin{bmatrix} \tau & 0 \\ 0 & \tau' \end{bmatrix} \text{ and } P = \begin{bmatrix} 1 & 1 \\ \tau & \tau' \end{bmatrix},$$

$$\text{so } P^{-1} = \frac{1}{\tau' - \tau} \begin{bmatrix} \tau' & -1 \\ -\tau & 1 \end{bmatrix}.$$

To obtain a closed form expression for u_n , compute

$$\begin{aligned} (\tau' - \tau)A^n &= \begin{bmatrix} 1 & 1 \\ \tau & \tau' \end{bmatrix} \begin{bmatrix} \tau^n & 0 \\ 0 & (\tau')^n \end{bmatrix} \begin{bmatrix} \tau' & -1 \\ -\tau & 1 \end{bmatrix} \\ &= \begin{bmatrix} \tau^n & (\tau')^n \\ * & * \end{bmatrix} \begin{bmatrix} * & -1 \\ * & 1 \end{bmatrix} = \begin{bmatrix} * & (\tau')^n - \tau^n \\ * & * \end{bmatrix} \end{aligned}$$

to show that

$$(2) \quad u_n = \frac{\tau^n - (\tau')^n}{\tau - \tau'}.$$

Finally, since $\tau, \tau' = (1 \pm \sqrt{5})/2$, we have

$$u_n = \frac{(1 + \sqrt{5})^n - (1 - \sqrt{5})^n}{2^n \sqrt{5}}.$$

Note how clean the calculation is when one ignores the numerical value of τ until the end.

- (a) Use relations (1) and the convention $\tau > 0$ to show that $|\tau'| < \tau$.
(b) Now use (2) to show that $\lim_{n \rightarrow \infty} (u_{n+1}/u_n) = \tau$. (None of this should require the numerical value of τ .)

4. Work a selection from Ireland and Rosen, Exercises 3.1, 3.4, 3.8–3.10, 3.12–3.13, 3.16, 3.17, 3.18, 3.23; do 3.24, 3.25, 3.26.