Mathematics 361: Number Theory
Assignment C

Reading: Ireland and Rosen, Chapter 3 (including the exercises) and into Chapter 4

Problems:

The pigeonhole principle and congruences.

1. Let m be a positive integer and $a_1, \ldots, a_m$ be any integers, possibly repeating. Show that for some nonempty subset S of the indices $\{1, \ldots, m\}$, $\sum_{i \in S} a_i \equiv 0 \pmod{m}$. (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 $(\mathbb{Z}/p\mathbb{Z})^\times$. 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 $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. 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 $\chi_A(\lambda) = \lambda^2 - \mathrm{tr}(A)\lambda + \det(A) = \lambda^2 - \lambda - 1$. We let τ and $\tilde{\tau}$ 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

$$\tau + \tilde{\tau} = 1, \qquad \tau\tilde{\tau} = -1. \tag{1}$$

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

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

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

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

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

To obtain a closed form expression for u_n, compute that $(\tilde{\tau} - \tau)A^n$ is

$$\begin{bmatrix} \tau & \tilde{\tau} \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \tau^n & 0 \\ 0 & \tilde{\tau}^n \end{bmatrix} \begin{bmatrix} 1 & -\tilde{\tau} \\ -1 & \tau \end{bmatrix} = \begin{bmatrix} * & * \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \tau^n & * \\ -\tilde{\tau}^n & * \end{bmatrix} = \begin{bmatrix} * & * \\ \tau^n - \tilde{\tau}^n & * \end{bmatrix},$$

and so

$$u_n = \frac{\tau^n - \tilde{\tau}^n}{\tau - \tilde{\tau}}. \tag{2}$$

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

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

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 $|\tilde{\tau}| < \tau$.

(b) Now use (2) to show that $\lim_{n\to\infty}(u_{n+1}/u_n) = \tau$. (None of (a) or (b) requires the numerical value of τ.)

4. Ireland and Rosen exercises 3.24, 3.25, 3.26. Note: 3.25 is technical; roughly λ is a square root of 3 and therefore a fourth root of 9, and so the condition $\alpha = 1\ (\lambda)$ suggests that $\alpha^3 = 1\ (\lambda^3)$, but the issue is to finagle one more power of λ to get to $\alpha^3 = 1\ (\lambda^4)$; and problem 3.24 can tell us that one of three elements must be a multiple of λ.

5. 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.

Optional alternate problems.

6. Use Hensel's Lemma to show that for distinct odd primes p and q, the 2-adic equation

$$px^2 + qy^2 = z^2, \quad x, y, z \in \mathbb{Z}_2$$

has a nonzero solution if at least one of p and q is 1 modulo 4 but not if both are 3 modulo 4.

7. Let $a, b \in \mathbb{Q}$ be nonzero. Show that the inhomogeneous condition

$$aX^2 + bY^2 = 1 \quad \text{has a solution in } \mathbb{Q}^2$$

and the homogeneous condition

$$aX^2 + bY^2 = Z^2 \quad \text{has a nonzero solution in } \mathbb{Z}^3$$

are equivalent.