Exercise 1. Construct a 2-paradoxical tournament on seven vertices. 

Hint: Use seven-fold rotational symmetry.

Exercise 2. Prove: \((\forall c \in (0,1)) \lim_{n \to \infty} n^k(1-c)^n = 0\). (Exponential decay beats polynomial growth.)

Exercise 3. The Legendre symbol is defined by

\[
\left(\frac{a}{p}\right) = \begin{cases} 
0 & \text{if } p \mid a \\
1 & \text{if } a \text{ is a quadratic residue mod } p \\
1 & \text{if } a \text{ is a non-residue mod } p 
\end{cases}
\]

where \(p\) is a prime. Show that \(\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)\).

Exercise 4. For which primes \(p\) is \(-1\) a quadratic non-residue mod \(p\)? Experiment with the first 25 primes and find a very simple formula. Prove your answer.

Exercise 5. Prove: if \(\exists a\) such that \(\gcd(a,N) = 1\) and

\[a^{N-1} \not\equiv 1 \pmod{N}\] (1)

then at least half the numbers relatively prime to \(N\) satisfy (1).

Exercise 6. If \(\gcd(a,b) = 1\) and \(p \mid a^2 + b^2\) then \(p \equiv 1 \pmod{4}\) or \(p = 2\).

Exercise 7. Prove that there are infinitely many primes \(\equiv 1 \pmod{4}\).

Exercise 8. Prove that there are infinitely many primes \(\equiv -1 \pmod{4}\).

Exercise 9. “\(\lim_{x \to 0^+, y \to 0^+} x^y = 1\) most of the time.”

Make sense of this statement and prove it.

Exercise 10. Make sense of the question “What is the probability that two random positive integers are relatively prime?” Prove that the answer is \(6/\pi^2\). 

\textit{Hint.} To prove that the required limit exists may be somewhat tedious. If you want to see the fun part, assume the existence of the limit, and prove in just two lines that the limit must be \(1/\zeta(2)\). \((\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \text{ is the “zeta function.”})\)
**Exercise 11.** Similarly prove that the probability that the gcd of three random numbers equals 1 is 1/ζ(3).

**Exercise 12.** Fix the proof, given in class, that Paley tournaments are $k$-paradoxical for $p > k^2 2^k$, so that it works without ignoring the case where $x \in A$.

**Exercise 13. Universal Graphs**
A graph $G$ is universal over all graphs with $k$ vertices (a $k$-universal graph) if all graphs with $k$ vertices are induced subgraphs of $G$. An easy example is simply the graph on $k2^{\binom{k}{2}}$ vertices obtained by taking the disjoint union of all graphs on $k$ vertices.

1. Prove that there exists a $k$-universal graph with $\leq ck^2$ vertices (for some constant $c$).

2. Construct an explicit example of size $\leq ck^2 4^k$.

**Exercise 14.** Let $U_k$ be a $k$-universal graph. Prove:

$$(\forall \epsilon > 0)(\exists k_0)(\forall k \geq k_0) (U_k \text{ must have } \geq (2 - \epsilon)k \text{ vertices.})$$

**Exercise 15. Pseudoprimes.** (Compare with Exercise 5.) A positive integer $N$ is a pseudoprime if for all integers $a$ that are relatively prime to $N$ we have $a^{N-1} \equiv 1 \pmod{N}$. (So these numbers satisfy Fermat’s little theorem and in this they behave “like primes.” Pseudoprimes are also called Carmichael numbers.) There are infinitely many pseudoprimes, but pseudoprimes are rare. If $N$ is composite but not a pseudoprime then it is easy to find a “witness” of the compositeness of $N$; half the integers $a$ between 1 and $N - 1$ that are relatively prime to $N$ violate Fermat’s little theorem. We find such an $a$ by random choice.

Proving compositeness of pseudoprimes is more difficult; handling them is the goal of the Solovay-Strassen primality test.

(a) Prove that if $N = pq$ where $p, q$ are distinct primes then $N$ is not a pseudoprime.

(b) Suppose $N = pqr$ where $p, q, r$ are distinct primes. Prove that $N$ is a pseudoprime if and only if $p - 1 | qr - 1$ and $q - 1 | pr - 1$ and $r - 1 | pq - 1$.

(c) Prove that 561 = 3 · 11 · 17 is a pseudoprime. (This is the smallest pseudoprime.)

(d) We want to find all pseudoprimes of the form $3pq$ where $p, q$ are distinct primes, $p, q \neq 3$. Prove that 561 is the only one.