Problem Set 2–Solutions

1. (a) Let \( Y = (X - \mathbb{E}[X] + b)^2 \) for some constant \( b > 0 \), we’ll optimize over \( b \) later.

\[
\Pr[X \geq \mathbb{E}[X] + a] = \Pr[X + b \geq \mathbb{E}[X] + a + b] \\
\leq \Pr[Y \geq (a + b)^2] \\
\leq \frac{\mathbb{E}[Y]}{(a + b)^2} \\
= \frac{\text{Var}[X] + b^2}{(a + b)^2}
\]

This is minimized by setting \( b = \frac{\text{Var}[X]}{a} \) giving our bound.

(b) For part (i) the one-sided inequality yields 0.3 while the two-sided bound yields 0.44. For part (ii) the one-sided inequality yields 0.1 while the two-sided bound yields 0.11. So for deviations close to the mean the one-sided inequality yields a considerable gain, but the gain goes down as we move farther from the mean.

2. Tightness of Markov’s and Chebyshev’s inequalities:

(a) A rather silly example is the random variable \( X \) that always takes value \( a \). \( \Pr[X \geq a] = 1 = \mathbb{E}[X] \). Other less-trivial constructions exist, for example, for \( a \geq 1 \), we could consider the random variable \( X \) defined by \( \Pr[X = a] = 1/a \) and \( \Pr[X = 0] = 1 - 1/a \), for which \( \Pr[X \geq a] = \mathbb{E}[X]/a \).

(b) The silly example would be the random variable \( X \) which takes value \(-a\) half the time, and value \( a \) half the time. A less silly example, for \( a \geq 1 \), is the random variable that takes value \( \pm a \) with probability \( 1/2a^2 \), and 0 with probability \( 1 - a^2 \). This random variable has variance 1, and \( \Pr[|X - \mathbb{E}[X]| \geq a] = 1/a^2 = \frac{\text{Var}[X]}{a^2} \).

3. Define the random variable \( Y = |X - \mathbb{E}[X]|^k \). Since \( Y \) is non-negative and \( a^k \) is positive, we can use Markov’s inequality to get the following:

\[
\Pr \left[ Y > a^k \left( \mathbb{E}[(X - \mathbb{E}[X])^k] \right) \right] = \Pr \left[ Y > a^k \left( \mathbb{E}[Y] \right) \right] \leq \frac{1}{a^k}.
\]

Note that we used the fact that \( k \) was even when we assumed \( (X - \mathbb{E}[X])^k = |X - \mathbb{E}[X]|^k \).

4. (a) The coefficient of \( x^k \) in the expansion of \( (x - a)^n \) is \( \binom{n}{k} a^{n-k} \). This binomial coefficient is always an integer, and for prime \( n \), the numerator of the binomial coefficient is a multiple of \( n \), and for \( k \in \{1, \ldots, n - 1\} \) the denominator has no factors of \( n \), as all the prime factors of the denominator are at most \( \max(k, n - k) \). Hence for \( n \) prime, \( (x - a)^n \cong x^n + (-a)^n \cong x^n - a^n \mod n \), where the final congruence used Fermat’s Little Theorem.

In the case that \( n \) is composite and not a power of a prime, we have \( n = p^k m \), for some prime \( p \) and \( m > 1 \) relatively prime to \( p \). Consider the coefficient of the \( x^{n-p^k} \) term:
\[ \frac{n!}{p^k[(n-p^k)]}a^{p^k} \]. Since \( \gcd(a,n) = 1 \), the \( a^{p^k} \) term has no factors of \( p \). Additionally, all factors of \( p \) in the numerator of the binomial coefficient are cancelled by factors of \( p \) in the denominator since \( p^k! \) and \( p^km \cdot (p^km - 1) \cdot \ldots \cdot p^k(m - 1) \) are divisible by the same power of \( p \); hence \( \frac{n!}{p^k[(n-p^k)]}a^{p^k} \not\equiv 0 \mod p \), and the polynomial \( (x - a)^n \mod p \) has a nonzero coefficient of \( x^{n-p^k} \).

(b) There are at least two reasons we cannot use the Schwartz-Zippel randomized test of polynomial identity to decide whether \( (x - 1)^n - (x^n - 1) \cong 0 \mod n \). The first reason is that this is a degree \( n - 1 \) polynomial, and hence could have at least \( n - 1 \) roots, yet the set from which we are selecting values to substitute for \( x \) has size \( |n| \), yielding an abysmal bound of \( 1/n \) on the probability of catching a composite. The second, more fundamental reason we cannot use Schwartz-Zippel is that in the case that \( n \) is composite, \( \mathbb{Z}_n^* \) is not a field, and hence even the polynomial ring modulo \( n \) has a number of problems—in particular, degree \( d \) polynomials may have more than \( d \) roots modulo \( n \). For example, the degree 2 polynomial \( p(x) = x^2 - x \) has the roots 1, 3, 4, 5 if we are working modulo 6.

(c) Assuming that \( n = p^km \) is composite, for \( m \geq 2 \) with \( \gcd(m,p) = 1 \), we will argue that with high probability over the random choice of \( r(x) \), \( q(x) = (x + 1)^n - (x^n + 1) \not\equiv 0 \mod (p, r(x)) \), and hence with at least with probability, this will hold modulo \( (n, r(x)) \), since \( p \) is a factor of \( n \). Because we are working modulo \( p \), polynomials have a unique factorization, and hence the degree \( n \) polynomial in question has at most \( n/d \) unique irreducible degree-\( d \) polynomial factors. We now argue that with a reasonable probability, \( r(x) \) will be an irreducible degree \( d \) polynomial that is not one of the irreducible degree \( d \) factors of \( q(x) \), in which case the algorithm will successfully verify that \( q(x) \neq 0 \). Using the bounds from the hint on the number of monic irreducible polynomials, and the fact that there are at most \( p^d \) monic degree \( d \) polynomials modulo \( p \) (and \( r(x) \mod p \) is chosen uniformly at randomly from among them, because it is chosen uniformly from degree \( d \) monic polynomials modulo \( n \) and \( p \) is a divisor of \( n \)), we have:

\[
\Pr[\text{success}] \geq \frac{p^d/d - p^{d/2} - n/d}{p^d} \geq \frac{1}{d} - \frac{1}{p^{d/2}} - \frac{n}{d \cdot 17 \log n} \geq \frac{1}{4d},
\]

where the last inequality is a very crude bound.