Problem 19
Bach Bui, Kevin Hughes, and Allison Moore

Problem 19 States: Prove that if $r > n/2$ and n is an r-AKS pseudoprime, then n is prime. Try to improve this inequality.

Let n be an r-AKS pseudoprime. Then n is odd number with $r \nmid n$, $r \nmid n^2 - 1$, and

$$(x+1)^n = x^n + 1 \bmod(n, x^r - 1)$$

Let us also state the condition that $p^2 \nmid n$. (This will be the Case 1; Case 2, for which $p^2 \mid n$ will be proved later). Thus, for some polynomial $t(x)$,

$$(x+1)^n - (x^n + 1) = (x^r - 1) \cdot t(x) \bmod(n)$$

$$\sum_{k=1}^{n-1} \binom{n}{k} x^k = (x^r - 1) \cdot t(x) \bmod(n)$$

$$\Rightarrow (x^r - 1) \mid \sum_{k=1}^{n-1} \binom{n}{k} x^k$$

Modding out by the polynomial $(x^r - 1)$ is equivalent to modding out by the relation $x^r \equiv 1$ mod(n). Thus for each x^ith term in the summation, the x^{i+r}th term is in the same equivalence class. Thus, the summation can be split into terms which have two elements in their equivalence class, and terms which have only one element in their class, which are the terms for which $i + r$ exceeds $n - 1$.

$$\sum_{k=1}^{n-1-r} (\binom{n}{k} x^k + \binom{n}{k+r} x^k) + \sum_{k=n-r}^{r} \binom{n}{k} x^k \equiv 0 \bmod(n)$$

For convenience, let $a_k = \binom{n}{k}$ or $(\binom{n}{k} + \binom{n}{k+r})$, depending on which summation it falls into. Then,

$$\sum_{k=1}^{n-1-r} (\binom{n}{k} x^k + \binom{n}{k+r} x^k) + \sum_{k=n-r}^{r} \binom{n}{k} x^k = \sum_{k=1}^{r} a_k x^k \equiv 0 \bmod(n)$$

The sum is congruent to 0 mod(n) $\Leftrightarrow$ each of the coefficients a_k is congruent to 0 mod n. In particular, consider $k = p$, where p is the smallest prime dividing n. Here we state a Lemma.

Lemma: Let p be the smallest prime divisor of composite n, $p = p_0$, where $n = p_0 \cdot p_1 \cdots p_j$. Then $\binom{n}{p} \not\equiv 0$ mod(n).

Proof: Assume $\binom{n}{p} \equiv 0$ mod(n). $\binom{n}{p} = \frac{n(n-1)\cdots(n-p+1)}{p(p-1)!}$. Since p is the smallest prime divisor of p, then $(p - i) \nmid n$, for all i $(1 \le i \le p - 1)$. Thus $p \mid n$ with $\frac{n}{p} = p_1 \cdots p_j$ and $\binom{n}{p} = (p_1 \cdots p_j) \cdot \frac{(n-1)\cdots(n-p+1)}{(p-1)!}$. Since $p_i \not\equiv n$ mod(n) for all i, $\Rightarrow \frac{(n-1)\cdots(n-p+1)}{(p-1)!} \equiv 0$ mod(n), but because $(p - i) \nmid n$ for all i $(1 \le i \le p - 1)$, then $\binom{n}{p} \not\equiv 0$ mod(n).

We may assume that $p \leq n-1-r$, that is, that p is in the first summation. Otherwise, we have that $\binom{n}{p} \equiv 0$ mod(n) $\Leftrightarrow \binom{n}{p} \equiv 0$ mod(p), which contradicts the lemma. So we have that:

$$\binom{n}{p} + \binom{n}{p+r} \equiv 0 \bmod(n)$$

And since $\binom{n}{p} \not\equiv 0$ mod(n),

$$\Rightarrow \binom{n}{p+r} \not\equiv 0 \bmod(n)$$

Now we will use the property of binomial coefficients, $k\binom{n}{k} = (n-k+1)\binom{n}{k-1}$, to rewrite $\binom{n}{p+r}$:

$$\binom{n}{p+r} = (\frac{1}{p+r})(n-(p+r)+1)\binom{n}{(p+r)-1}$$

$$= \frac{(n-(p+r)+1)n!}{(p+r)!(n-(p+r))!}$$

$$= \frac{(n-(p+r)+1)(n-(p+r))\cdots(n-p)n!}{(p+r)\cdots(p+1)p!(n-p)!}$$

$$= \frac{(n-p-r+1)(n-p-r)\cdots(n-p)}{(p+r)\cdots(p+1)}\binom{n}{p}$$

And since it is known that $\binom{n}{p} \not\equiv 0$ mod(n), then we may assume that

$$\equiv \frac{(n-(p+r)+1)(n-(p+r))\cdots(n-p)}{(p+r)\cdots(p+1)} \text{ mod(p)}$$

Here we will state and apply Wilson's Theorem. Wilson's Theorem: $(p-1)! \equiv -1$ mod(p). Thus, modulo p we can regroup and factor out $p! = p(p-1)! \equiv p(p-1)$ mod(p), from the numerator and the denominator. We can rewrite the product in more convenient form:

$$\frac{(n-p-r+1)(n-p-r+1+1)\cdots(n-p-r+1+(p-1))(n-p-r+1+p)\cdots(n-p)}{(p+r)\cdots(2p+1)(2p)(2p-1)\cdots(p+2)(p+1)} \not\equiv 0 \text{ mod(n)}$$

$$= \frac{(n-p-r+1)(n-p-r+1+1)\cdots(n-p-r+1+(p-1))}{(2p)(2p-1)\cdots(p+2)(p+1)} \cdot \frac{(n-p-r+1+p)\cdots(n-p)}{(p+r)\cdots(2p+1)}$$

$$\equiv \frac{p(p+1)(p+2)\cdots(p-1)}{p(p-1)\cdots(2)(1)} \cdot \frac{(n-p-r+1+p)\cdots(n-p)}{(p+r)\cdots(2p+1)} \text{ mod(p)}$$

$$\equiv \frac{p(p-1)!}{p(p-1)!} \cdot \frac{(n-p-r+1+p)\cdots(n-p)}{(p+r)\cdots(2p+1)} \text{ mod(p)}$$

$$\equiv \frac{(n-p-r+1+p)\cdots(n-p)}{(p+r)\cdots(2p+1)} \text{ mod(p)}$$

$$\equiv \frac{(n-r+1)\cdots(n-p)}{(p+r)\cdots(2p+1)} \text{ mod(p)}$$

Now note that this same trick can be applied again. In fact, it can be applied s times, where $s = \lfloor \frac{r}{p} \rfloor$, the number of times that $p \mid r$. Thus, after s iterations, we are left with:

$$\equiv \frac{(n-p-r+1+sp)\cdots(n-p)}{(p+r)\cdots((s+1)p+1)} \text{ mod(p)}$$

$$\equiv \frac{(n-r+1+(s-1)p)\cdots(n-p)}{(p+r)\cdots((s+1)p+1)} \text{ mod(p)}$$

Let $X = \frac{(n-r+1+(s-1)p)\cdots(n-p)}{(p+r)\cdots((s+1)p+1)}$. The number of terms in the denominator is strictly less than p, with none of them congruent to p mod(p). Since p is prime, then none of the terms divide p. Thus,

$$\Rightarrow X \equiv 0 \text{ mod(p)}$$

And since we are working in the case for wich $p^2 \nmid n$, then

$$\Rightarrow X\binom{n}{p} \equiv 0 \text{ mod(n)}$$

And so we have that

$$\binom{n}{p+r} + \binom{n}{p} = \underbrace{X\binom{n}{p}}_{\equiv 0 \text{ mod(n)}} + \underbrace{\binom{n}{p}}_{\not\equiv 0 \text{ mod(n)}} \not\equiv 0 \text{ mod(n)}$$

But we had assumed that $\binom{n}{p+r} + \binom{n}{p} \equiv 0$ mod(n), which is a contradiction. Therefore, since the sum

$$\sum_{k=1}^{r} a_k x^k \equiv 0 \text{ mod}(n)$$

and since there exists a paired term a_k for which $a_k \not\equiv 0$ when n is composite, it is left to conclude that each binomial coefficient $\binom{n}{k} \equiv 0$ for all $k, 1 \leq k \leq n-1$. And then

$$\binom{n}{k} \equiv 0 \ \forall k, 1 \leq k \leq n-1 \Leftrightarrow \text{ n is prime.}$$

Improve the inequality.

Rather than the condition $r > n/2$, we will try to employ the condition $r > n/q$ for $q > 2$. First, observe the case when $q = 3$.

$r > n/3$

When we reduce modulo the relation $x^r \equiv 1$ mod(n), we are left with the split summation:

$$\sum_{k=1}^{n-2r-1} (\binom{n}{k} + \binom{n}{k+r})x^k + \sum_{k=n-2r}^{r} (\binom{n}{k} + \binom{n}{k+r} + \binom{n}{k+2r})x^k \equiv 0 \text{ mod}(n)$$

where $r > n/3$ and $2 = \lfloor \frac{n}{r} \rfloor$. Again, we consider p such that p is the smallest prime divisor of n. We assume that the coefficient $\binom{n}{p}$ occurs in the second summation, otherwise, we reduce the problem to the previously solved case. We assume that:

$$(\binom{n}{p} + \binom{n}{p+r} + \binom{n}{p+2r}) \not\equiv 0 \bmod(n)$$

Since we know that $\binom{n}{p} \not\equiv 0$ mod(n), we assume $(\binom{n}{p+r} + \binom{n}{p+2r}) \not\equiv 0$ mod(n). Then, applying the same procedure as before, we reduce the two binomial coefficients by grouping together and cancelling out the terms $p(p-1)!$ mod(p), s_1 and s_2 times, respectively. ($s_1 = \lfloor \frac{r}{p} \rfloor$ and $s_2 = \lfloor \frac{2r}{p} \rfloor$).

$$(\binom{n}{p} + \binom{n}{p+r} + \binom{n}{p+2r}) \equiv 0 \bmod(n)$$

$$= \cdots = \frac{(n-p-r+1)(n-p-r)\cdots(n-p)}{(p+r)\cdots(p+1)}\binom{n}{p} + \frac{(n-p-2r+1)(n-p-2r)\cdots(n-p)}{(p+2r)\cdots(p+1)}\binom{n}{p}$$

$$= \frac{(n-(p+r)+1)(n-(p+r))\cdots(n-p)}{(p+r)\cdots(p+1)} + \frac{(n-(p+2r)+1)(n-(p+2r))\cdots(n-p)}{(p+2r)\cdots(p+1)} \text{ mod(p)}$$

$$\equiv \frac{(n-p-r+1+s_1p)\cdots(n-p)}{(p+r)\cdots((s_1+1)p+1)} + \frac{(n-p-2r+1+s_2p)\cdots(n-p)}{(p+2r)\cdots((s_2+1)p+1)} \text{ mod(p)}$$

$$\equiv \frac{(n-r+1+(s_1-1)p)\cdots(n-p)}{(p+r)\cdots((s_1+1)p+1)} + \frac{(n-2r+1+(s_2-1)p)\cdots(n-p)}{(p+2r)\cdots((s_2+1)p+1)} \text{ mod(p)}$$

Where $2r = (s_1+1)p + q_1$ and $2r = (s_2+1)p + q_2$ for some integers $q_1, q_2 < p$. Also, we have that $q_1, q_2 > 0$. This is true because

$$q_1 = q_2 = 0 \Leftrightarrow (s_1+1)p = r \text{ and}(s_2+1)p = 2r \Leftrightarrow (s_1+1) = 1 \text{ and}(s_2+1) \mid 2$$

$$\Leftrightarrow s_1 = 0 \text{ and}s_2 = 1 \Leftrightarrow p = r$$

But $p \nmid r$ since r is a prime, and $p \neq r$ since $r \nmid n$. So $q_1, q_2 > 0$. Thus all the terms of the bottom are distinct congruence classes mod(p), with none congruent to p. Therefore, let:

$$X_1 = \frac{(n-r+1+(s_1-1)p)\cdots(n-p)}{(p+r)\cdots((s_1+1)p+1)}$$

$$X_2 = \frac{(n-2r+1+(s_2-1)p)\cdots(n-p)}{(p+2r)\cdots((s_2+1)p+1)} \text{ mod(p)}$$

where X_1 and X_2 are each congruent to 0 mod(p), since no terms in the denominators divide their numerators. Thus,

$$\Rightarrow X_1\binom{n}{p} + X_2\binom{n}{p} + \binom{n}{p} \equiv 0 \text{ mod(p)}$$

$$\Rightarrow (\underbrace{X_1}_{\equiv 0} + \underbrace{X_2}_{\equiv 0} + 1)\underbrace{\binom{n}{p}}_{\not\equiv 0}$$

$$\Rightarrow (X_1 + X_2 + 1)\binom{n}{p} \not\equiv 0 \text{ mod(p)}$$

$$\Rightarrow (X_1 + X_2 + 1)\binom{n}{p} \not\equiv 0 \text{ mod(n)}$$

And again, this is a contradiction because we had previously assumed that all coefficients $a_i \equiv 0$ mod(n). Thus, since there is no way summing binomial coefficients to be $\equiv 0$ mod(n), then we must conclude that each binomial coefficient $\binom{n}{k} \equiv 0$ mod(n) $\Leftrightarrow n$ is prime.

$r > n/q$
Now when we reduce modulo the relation $x^r \equiv 1$ mod(n), we are left with the split summation:

$$\sum_{k=1}^{n-qr-1} (\binom{n}{k} + \cdots + \binom{n}{k+ir})x^k + \sum_{k=n-2r}^{r} (\binom{n}{k} + \cdots + \binom{n}{k+(i-1)r})x^k \equiv 0 \text{ mod}(n)$$

where i is the floor of number of times that r divides n, $i = \lfloor \frac{n}{r} \rfloor$. Let p be the smallest prime divisor of n and assume that the coefficient $\binom{n}{p}$ occurs in the first summation, otherwise, we reduce the problem to the previously solved case. We assume that:

$$(\binom{n}{p} + \binom{n}{p+r} + \cdots + \binom{n}{p+ir}) \not\equiv 0 \text{ mod}(n)$$

Since we know that $\binom{n}{p} \not\equiv 0$ mod(n), we assume $(\binom{n}{p+r} + \cdots + \binom{n}{p+ir}) \not\equiv 0$ mod(n). Then, applying the same procedure as before, we reduce the set of binomial coefficients by grouping together and cancelling out the terms $p(p-1)!$ mod(p), s_j times, where $s_j = \lfloor \frac{jr}{p} \rfloor$, $l \leq j \leq i$. Then,

$$(\binom{n}{p} + \binom{n}{p+r} + \cdots + \binom{n}{p+ir}) \not\equiv 0 \text{ mod}(n)$$

$$= \cdots = \frac{(n-p-r+1)(n-p-r)\cdots(n-p)}{(p+r)\cdots(p+1)}\binom{n}{p} + \cdots + \frac{(n-p-ir+1)(n-p-ir)\cdots(n-p)}{(p+ir)\cdots(p+1)}\binom{n}{p}$$

$$= \frac{(n-(p+r)+1)(n-(p+r))\cdots(n-p)}{(p+r)\cdots(p+1)} + \cdots + \frac{(n-(p+ir)+1)(n-(p+ir))\cdots(n-p)}{(p+ir)\cdots(p+1)} \text{ mod(p)}$$

$$\equiv \frac{(n-p-r+1+s_1p)\cdots(n-p)}{(p+r)\cdots((s_1+1)p+1)} + \cdots + \frac{(n-p-ir+1+s_ip)\cdots(n-p)}{(p+ir)\cdots((s_i+1)p+1)} \text{ mod(p)}$$

$$\equiv \frac{(n-r+1+(s_1-1)p)\cdots(n-p)}{(p+r)\cdots((s_1+1)p+1)} + \cdots + \frac{(n-ir+1+(s_i-1)p)\cdots(n-p)}{(p+ir)\cdots((s_i+1)p+1)} \text{ mod(p)}$$

Where $jr = (s_j+1)p + q_j$ for some integer $q_j, q_j < p$. Further, let:

$$X_j = \frac{(n-jr+1+(s_j-1)p)\cdots(n-p)}{(p+jr)\cdots((s_j+1)p+1)} \quad l \leq j \leq i$$

Now here we should note several things.

1. Since r is a prime, $p \nmid r$, and $p \neq r$ since $p \mid n$ and $r \nmid n$. Thus, $q_j > 0$.

2. We want to be sure that the denominator is not congruent to 0 mod(p). If we look at the denominator of X_j as a function of p, we can write it as

$$(p + jr) \cdots (p + 1) = f(p) + C = f(p) + (jr)!$$

where the constant term C is the factorial $(jr)!$, which has terms divisible by p. However, many of those terms will cancel mod(p), and if we rewrite the denominator as a function of $(s + 1)p$ after grouping terms mod(p) we get:

$$(p + jr) \cdots ((s_j + 1)p + 1) = (p + (s_j p + q_j)) \cdots ((s_j + 1)p + 1) = ((s_j + 1)p + q_j) \cdots ((s_j + 1)p + 1)$$
$$= f((s_j + 1)p) + C = f((s_j + 1)p) + (q_j)!$$

where $q_j < p$.

3. If $q_j \neq 0$, then we can be sure that each term in the factorial is a distinct nonzero congruence class mod(p). And since:

$$q_j = 0 \Leftrightarrow s_j = \frac{jr}{p} \Leftrightarrow s_j p = jr \Leftrightarrow p \mid j$$

And when $p \mid j$, we have that $X_j \equiv 1$ mod(p), whereas when $p \nmid j$, we have that $X_j \equiv 0$ mod(p). We need to count the number of times t that $p \mid j$, $t = \lfloor \frac{i}{p} \rfloor$.

Thus we redo the bound. Suppose $r > n/p(p - 1)$. Then

$$i < p(p - 1) \Rightarrow t = \lfloor \frac{i}{p} \rfloor < p - 1 \Rightarrow t + 1 < p - 1 + 1 = p$$

Thus t is a nonzero congruence class mod(p) so that:

$$X_1 \binom{n}{p} + X_2 \binom{n}{p} + \cdots + X_i \binom{n}{p} + \binom{n}{p}$$
$$\equiv (X_1 + X_2 + \cdots + X_i + 1) \binom{n}{p}$$
$$\equiv (\underbrace{t}_{<p-1} + 1) \underbrace{\binom{n}{p}}_{\not\equiv 0} \not\equiv 0 \text{ mod(p)}$$
$$\equiv (\underbrace{t + 1}_{\not\equiv 0}) \underbrace{\binom{n}{p}}_{\not\equiv 0} \not\equiv 0 \text{ mod(n)}$$

And again, this is a contradiction because we had previously assumed that all coefficients $a_i \equiv 0$ mod(n). Thus, since there is no way summing binomial coefficients to be $\equiv 0$ mod(n), then we must conclude that each binomial coefficient $\binom{n}{k} \equiv 0$ mod(n) $\Leftrightarrow n$ is prime, specifically when $r > n/p(p - 1)$.