Products of Factorials Modulo p

Florian Luca [1] *and* *Pantelimon Stănică* [2] *

[1] IMATE, UNAM, Ap. Postal 61-3 (Xangari), CP. 58 089
Morelia, Michoacán, Mexico; e-mail: fluca@matmor.unam.mx
[2] Auburn University Montgomery, Department of Mathematics,
Montgomery, AL 36124-4023, USA; e-mail: stanica@sciences.aum.edu

January 21, 2003

1 Introduction

Let p be a fixed odd prime and let s and t be fixed positive integers which depend on p. Consider the following subset of the elements of $\mathbf{Z}_p^*$

$$P_{s,t}(p) = \{x_1! \cdot x_2! \cdot \cdots \cdot x_t! \pmod p \mid x_i \geq 1 \text{ for } i = 1,\ 2,\ \ldots,\ t, \text{ and } \sum_{i=1}^{t} x_i = s\}. \quad (1)$$

The problem that we investigate in this note is the following: given p, find sufficient conditions that the parameters s and t should satisfy such as to ensure that $P_{s,t}(p)$ contains the entire $\mathbf{Z}_p^*$.
Let $\varepsilon > 0$ be any small number. Throughout this paper, we denote by $c_1,\ c_2,\ \ldots$ computable positive constants which are either absolute or depend on ε. From the way we formulated the above problem, we see that its answer is easily decidable if either both s and t are very small (with respect to p) or very large with respect to p. For example, if $s < c_1(\log(p))^2$ with some suitable constant c_1, then it is clear that $P_{s,t}(p)$, or even the union of all $P_{s,t}(p)$ for all allowable values of t, cannot possibly contain the entire $\mathbf{Z}_p^*$ when p is large. Indeed, the reason here is that the cardinality of the union of all $P_{s,t}(p)$ for all allowable values of t is at most $p(s) = O(\exp(c_2\sqrt{s}))$ and this is much smaller than p when p is large if c_1 is chosen such that $c_1 > c_2^2$. Here, we denoted by $p(s)$ the number of unrestricted partitions of s, and the constant c_2 can be chosen to be equal to $\pi\sqrt{\frac{2}{3}}$.
It is also obvious that $P_{s,t}(p)$ does not generate the entire $\mathbf{Z}_p^*$ (for any s) when $t = 2$. Moreover, the fact that there exist infinitely many prime numbers p for which the smallest nonquadratic residue modulo p is at least $c_3 \log(p)$, shows that if one wants to generate

*Also Associated to the Institute of Mathematics of Romanian Academy, Bucharest, Romania the entire $\mathbf{Z}_p^*$ out of $P_{s,t}(p)$, then one should allow in (1) partitions of s where $\max(x_i)_{i=1}^t$ is at least $c_3\log(p)$. In particular, s and t cannot be too close to each other. Indeed, if p is such a prime and the maximum value of the x_i's allowed in (1) is at most $c_3\log(p)$, then all the numbers in $P_{s,t}(p)$ will be quadratic residues modulo p, and in particular $P_{s,t}(p)$ cannot contain the entire $\mathbf{Z}_p^*$. On the other hand, when s is very large, for example when $s > p^{5/4+\varepsilon}$, then an immediate argument based on the known upper bounds for the size of the smallest primitive root modulo p shows that the union of $P_{s,t}(p)$ over all the allowable values of the parameter t does cover the entire $\mathbf{Z}_p^*$ when p is large. Thus, the question becomes interesting when we search for *small* values of both s and t for which $P_{s,t}(p)$ does cover the entire $\mathbf{Z}_p^*$.

This question was inspired by the paper of the second author [9]. In that paper, the problem investigated was the exponent at which a prime number p divides some generalized Catalan numbers. However, the question of whether a certain subset of Catalan numbers, namely the numbers of the form

$$\frac{1}{p}\cdot\binom{p}{m_1, m_2, \ldots, m_t} \tag{2}$$

covers the entire $\mathbf{Z}_p^*$ was not investigated in [9]. Here, the numbers appearing in (2) are all the nontrivial multinomial coefficients. In our notation, this question reduces to whether or not

$$\bigcup_{t\geq 2} P_{p,t}(p) \tag{3}$$

is the entire $\mathbf{Z}_p^*$. Allowing also $t = 1$ in (3) we obtain that even $0 \in \mathbf{Z}_p$ belongs to this set, and $s = p$ is the smallest value of s for which this can happen. As a byproduct of our results, we show that the set (3) is indeed the entire $\mathbf{Z}_p^*$, for $p \neq 5$.

Our main results are the following:

Theorem 1.
Let $\varepsilon > 0$ be arbitrary. There exists a computable positive constant $p_0(\varepsilon)$ such that whenever $p > p_0(\varepsilon)$, then $P_{s,t}(p) = \mathbf{Z}_p^*$ for all t and s such that $t > p^{\varepsilon}$ and $s - t > p^{1/2+\varepsilon}$.

The above result is certainly very far from best possible. We believe that the exponent $1/2$ appearing at the power of p in the lower bound for $s - t$ can be replaced by a much smaller one, or even maybe that the statement of Theorem 1 above remains true when $s - t > p^{2\varepsilon}$. We have not been able to find an argument to prove such a claim.

Theorem 2.
The set (3) is the entire $\mathbf{Z}_p^*$, if $p \neq 5$ is prime.

The trick in proving Theorem 2 is to detect a small value of p_0 such that Theorem 2 holds for $p > p_0$, and then to test the claim for all prime numbers p from 2 up to p_0.

Theorem 1 above shows, in particular, that the set (3) (even a very small subset of it) is the entire $\mathbf{Z}_p^*$ when p is large. As an example for Theorem 1, we can easily prove that if 2 is a primitive root modulo p, then $A \cup B$, where

$$A = \left\{ 2^u \left(\frac{p-1}{2} \right)! \,|\, 1 \le u \le \frac{p-1}{2} \right\}$$
$$B = \left\{ 2^v \left(\frac{p-3}{2} \right)! \,|\, 0 \le v \le \frac{p-3}{2} \right\}$$

cover the entire $\mathbf{Z}_p^*$. We see first that A and B each contain $\frac{p-1}{2}$ distinct residues modulo p. The intersection $A \cap B$ is empty, when 2 is a primitive root modulo p. We omit the details. What is interesting is that, in general, we can cover easily all the even residues, and the odd residues from the first half of $\mathbf{Z}_p^*$, since

$$\frac{1}{p}\binom{p}{2, 2k-1, p-2k-1} \equiv k \pmod{p}$$
$$\frac{1}{p}\binom{p}{1, 1, 2k-1, p-2k-1} \equiv 2k \pmod{p},$$

for any $1 \le k \le \frac{p-1}{2}$.
Related to our work, we recall that the behavior of the sequence $n! \pmod{p}$ was recently investigated in [2].

2 The Proofs of the Theorems

The main idea behind the proofs of both Theorems 1 and 2 is to find a suitable list $x_1,\ x_2,\ \ldots,\ x_t$ consisting of many small numbers and each one of them repeated a suitable number of times, such that we can modify (in a sense that will be made precise below) the fixed element given by formula (1) for this list of elements $x_1,\ x_2,\ \ldots,\ x_t$ in enough ways (such that, of course, these modified numbers do not get outside $P_{s,t}(p)$) so that to ensure that in the end, we have obtained all the congruence classes in $\mathbf{Z}_p^*$.
Here is the basic operation by which we can modify a fixed element, call it

$$F := \prod_{i=1}^{t} x_i!$$

in such a way as to obtain, hopefully, new elements in $P_{s,t}(p)$.
(M) *Assume that $i_1 < i_2 < \cdots < i_j$ and $l_1 < l_2 < \cdots < l_j$ are two disjoints subsets of indices in $\{1,\ 2,\ \ldots,\ t\}$. Then,*

$$\Big(\prod_{s=1}^{j}(x_{l_s}+1)\Big)\Big(\prod_{s=1}^{j} x_{i_s}\Big)^{-1} \cdot F = x_1! \cdots (x_{l_1}+1)! \cdots (x_{i_1}-1)! \cdots x_t! = F' \in P_{s,t}(p). \quad (4)$$

In general, we shall always apply formula (4) with $x_{l_1} = \cdots = x_{l_j} = 1$. With this convention, we may eliminate the initial number F, take inverses in (4) above, and then reformulate the question as follows:

Question: *Is it true that for suitable integers t and s (satisfying, for example, the hypothesis of Theorem 1) we can find some positive integers $x_1,\ x_2,\ \ldots,\ x_t$ summing to s, such that every nonzero residue class modulo p can be represented by a number of the form*

$$\prod_{r=1}^{j}\binom{x_{i_r}}{2} \tag{5}$$

where a subset of indices $\{i_1,\ i_2,\ \ldots,\ i_j\}$ of $\{1,\ 2,\ \ldots,\ t\}$ in (5) can be any subset as long as there exists another subset of j indices $\{l_1,\ l_2,\ \ldots,\ l_j\}$ disjoint from $\{i_1,\ i_2,\ \ldots,\ i_j\}$ for which $x_{l_r}=1$ for all $r=1,\ 2,\ \ldots,\ j$?

The Proof of Theorem 1. All we have to show is that if the parameters s and t satisfy the hypothesis of Theorem 1, then we can construct a list of elements $x_1,\ x_2,\ \ldots,\ x_t$ for which the answer to the above question is affirmative. Fix $\varepsilon>0$ and a positive integer k with $\frac{1}{k}<\varepsilon<\frac{2}{k}$. From now on, all positive constants $c_1,\ c_2,\ \ldots,$ which will appear will be computable and will depend only on k. We shall show that if p is large enough with respect to k, then we can construct a good sublist of numbers $x_1,\ x_2,\ \ldots,\ x_t$ in the following manner:

1) *We first take and repeat exactly two times each of the prime numbers x_i up to $p^{1/k}$.*

2) *We then adjoin some even numbers x_j, each one of them smaller than $p^{1/2+1/k}$ but such that the totality of those (counted with multiplicities) does not exceed $c_1\log(\log(p))$.*

3) *The numbers of the form (5), where the x_i's are from the lists 1 and 2 and the maximum length j of a product in (5) is not more than $2k+2c_1\log(\log(p))$ cover the entire $\mathbf{Z}_p^*$.*

It is clear that if we can prove the existence of a list satisfying 1)–3) above, then we are done. Indeed, we may first adjoin at the sublist consisting of the numbers appearing at 1) and 2) above a number of about $2k+2c_1\log(\log(p))$ values of x_i all of them equal to 1. The totality of all these numbers (the ones from 1), 2) and these new values of x_i all equal to 1) counted with their multiplicities, so far, is certainly not more than

$$c_2\frac{p^{1/k}}{\log(p)}+2k+4c_1\log(\log(p))<p^{\varepsilon}-1<t-1, \tag{6}$$

while their sum is at most

$$c_3\frac{p^{2/k}}{\log(p)}+2k+2c_1\log(\log(p))+2c_1\log(\log(p))p^{1/2+1/k}<p^{1/2+\varepsilon}-1<s-t-1, \tag{7}$$

for large p. At this step, we may finally complete the above list with several other values of the x_i equal to 1 until we get a list with precisely $t-1$ numbers, which is possible by inequality (6) above, and set the last number of the list to be equal to

$$x_t:=s-\sum_{i=1}^{t-1}x_i,$$

which is still positive by inequality (7) above.

To show the existence of a sublist with properties 1)–3) above, we start with the set

$$A := \{n \mid n < p^{1/k} \text{ and } n \text{ is prime}\}.$$

The numbers from A will form the sublist mentioned at 1) above but, so far, we take each one of them exactly once. Let

$$B_1 := \left\{ \frac{n_1}{2} \cdot \frac{n_2}{2} \cdot \dots \cdot \frac{n_k}{2} \;\Big|\; n_i \in A,\ n_i \neq n_j \text{ for } 1 \le i \neq j \le k \right\}.$$

We first notice that each value of $n \in A$ appears at most k times in an arbitrary product in B_1. We now show that $b_1 := \#B_1$ is large. Indeed, the set B_1 will certainly contain all the numbers of the form

$$\frac{p_1}{2} \cdot \frac{p_2}{2} \cdot \dots \cdot \frac{p_k}{2} = 2^{-k} \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k, \tag{8}$$

where p_i is an arbitrary prime subject to the condition

$$p_i \in \left(\frac{p^{1/k}}{2^i},\ \frac{p^{1/k}}{2^{i-1}} \right) \qquad \text{for } i = 1,\ 2,\ \dots,\ k. \tag{9}$$

Moreover, notice that the residue classes modulo p of the elements of the form (8), where the primes p_i satisfy conditions (9), are all distinct. Indeed, the point is that if two of the numbers of the form (8) coincide modulo p, then, after cancelling the factor of 2^{-k}, we get two residue classes of integers which coincide modulo p. Now each one of these two integers is smaller than p, therefore if they coincide modulo p, then they must be, in fact, equal. Now the fact that they are all distinct follows from the fact that their prime divisors p_i satisfy condition (9). Applying the Prime Number Theorem to estimate from below the number of primes in each one of the intervals appearing in formula (9), we get

$$b_1 > c_4 \frac{p}{(\log(p))^k} > \frac{p}{(\log(p))^{k+1}}, \tag{10}$$

whenever $p > c_5$. We construct recursively a (finite) increasing sequence of subsets B_m for $m \ge 1$ in the following way:

Assume that B_m has been constructed and set $b_m := \#B_m$. Assume that $b_m < p-1$ (that is, B_m is not the entire $\mathbf{Z}_p^*$ already). We then have the following trichotomy:

i) If $b_m \ge p/2$, we then set $B_{m+1} := B_m \cdot B_m$, and notice that $B_{m+1} = \mathbf{Z}_p^*$ and we can no longer continue.

ii) If $b_m < p/2$ and there exists an even number $a < p^{1/2+1/k}$ such that $a/2 \notin B_m \cdot B_m^{-1}$, we then set $a_m := a$, add a to the list of the x_i's (as one of the numbers from sublist 2) above), and we let

$$B_{m+1} := B_m \cup \frac{a_m}{2} \cdot B_m.$$

Notice that

$$b_{m+1} \ge 2b_m. \tag{11}$$

iii) If $b_m < p/2$ and all even numbers a up to $p^{1/2+1/k}$ have the property that $a/2$ is already in $B_m \cdot B_m^{-1}$, we choose the even number a smaller than $p^{1/2+1/k}$ for which the number of representations of $a/2$ of the form $x \cdot y^{-1}$ with $x,\ y \in B_m$ is minimal. We then set $a_m := a$, add a to the list of the x_i's (as one of the numbers from sublist 2) above), set

$$B_{m+1} := B_m \cup \frac{a_m}{2} \cdot B_m,$$

and notice that

$$b_{m+1} \geq \frac{4b_m}{3}. \tag{12}$$

In i)–iii) above we have used the set-theoretic notation, namely that if U and V are two subsets of $\mathbf{Z}_p^*$, we have denoted by $U \cdot V$ the set of all elements of $\mathbf{Z}_p^*$ of the form $u \cdot v$ with $u \in U$ and $v \in V$, and by U^{-1} the set of all elements of the form u^{-1} for $u \in U$.
We have to justify that i)–iii) above do indeed hold. Notice that i) and ii) are obvious. The only detail we have to justify is that inequality (12) indeed holds in situation iii). For this, we use the following result due to Sárkőzy (see [7]):

Lemma 1.
Let p be a prime number, $u,\ v,\ S,\ T$ be integers with $1 \leq u,\ v \leq p-1,\ 1 \leq T \leq p$, furthermore $C_1,\ C_2,\ \ldots,\ C_u$ and $D_1,\ D_2,\ \ldots,\ D_v$ are integers with

$$C_i \not\equiv C_j \pmod{p}, \quad \text{for } 1 \leq i < j \leq u,$$

and

$$D_i \not\equiv D_j \pmod{p}, \quad \text{for } 1 \leq i < j \leq v.$$

For any integer n, let $f(n)$ denote the number of solutions of

$$C_x \cdot D_y \equiv n \pmod{p}, \quad 1 \leq x \leq u,\ 1 \leq y \leq v.$$

Then,

$$\Big| \sum_{n=S+1}^{S+T} f(n) - \frac{uvT}{p} \Big| < 2(puv)^{1/2}\log(p). \tag{13}$$

We apply Lemma 1 above with $u = v = b_m$, $C_1,\ C_2,\ \ldots,\ C_u$ all the residue classes in B_m and $D_1,\ D_2,\ \ldots,\ D_u$ all the residue classes in B_m^{-1}. We also set $S = 0$ and T to be the largest integer smaller than $p^{1/2+1/k}/2$. Clearly, $T > p^{1/2+1/k}/3$. Since we are discussing situation iii) above, we certainly have $f(n) \geq 1$ for all positive integers n up to T. Let $M := \min(f(n) \mid 1 \leq n \leq T)$, and then $a_m := 2c$, where $f(c) = M$. Denote b_m by b. We apply inequality (13) to get

$$M < \frac{b^2}{p} + \frac{2b\sqrt{p}\log(p)}{T}. \tag{14}$$

We first show that the inequality

$$\frac{2b\sqrt{p}\log(p)}{T} < \frac{b^2}{3p} \tag{15}$$

holds. Indeed, since $T > p^{1/2+1/k}/3$ and $b = b_m \geq b_1 > \dfrac{p}{(\log(p))^{k+1}}$ (by inequality (10)), it follows that in order for (15) to hold, it suffices that

$$54(\log(p))^{k+2} < p^{1/k},$$

which is certainly satisfied when $p > c_6$. Thus, inequalities (14) and (15) show that

$$M < \frac{4b^2}{3p} < \frac{2b}{3}, \tag{16}$$

where the last inequality in (16) follows because $b < p/2$. In particular,

$$b_{m+1} = \#(B_m \cup c \cdot B_m) \geq b_m + (b_m - M) \geq 2b - \frac{2b}{3} = \frac{4b}{3}, \tag{17}$$

which proves inequality (12).
The combination of (10), (11) and (12) shows that

$$b_{m+1} > \left(\frac{4}{3}\right)^m b_1 > \left(\frac{4}{3}\right)^m \frac{p}{(\log(p))^{k+1}} \tag{18}$$

holds as long as $b_m < p/2$. Now notice that the inequality

$$\left(\frac{4}{3}\right)^m > \frac{(\log(p))^{k+1}}{2}$$

will happen provided that $m > c_7 \log(\log(p))$, where one can take $c_7 := \dfrac{k+1}{\log(4/3)}$, for example, and for such large m inequality (18) shows that $b_{m+1} > p/2$. In particular, situations ii) or iii) above will not occur for more than $c_7 \log(\log(p))$ steps after which we arrive at a point where we apply situation i) to construct B_{m+1} and we are done. Clearly, i)–iii) and the above arguments prove the existence of a sublist of the x_i's satisfying conditions 1)–3), which finishes the proof of Theorem 1.

The Proof of Theorem 2. We follow the method outlined in the proof of Theorem 1. Thus, it suffices to find a list of positive integers, say $A := \{x_1,\ x_2,\ \ldots,\ x_s\}$, with

$$U := \sum_{i=1}^{s} x_i < p,$$

and such that for every $m \in \mathbf{Z}_p^*$ there exists a subset $I \subseteq \{1,\ 2,\ \ldots,\ s\}$ for which

$$m \equiv \prod_{i \in I} x_i\,! \pmod{p}.$$

It is clear that once we show the existence of such a list A so that every nonzero residue class m modulo p has a representation as shown above, we can then formally multiply the number appearing in the right hand side of the above congruence by an appropriate number of 1! so that to insure that the sum of the positive integers x_i for $i \in I$ and the 1's, the product of whose factorials is still m modulo p, is precisely p.

Step 1. We start with a set A_1 of distinct positive integers such that

$$U_1 := \sum_{x \in A_1} x$$

is not too large, and set

$$B_1 := \left\{ \frac{n_1}{2} \cdot \frac{n_2}{2} \;\middle|\; n_1 < n_2 \text{ in } A_1 \right\} \pmod p.$$

For $m \geq 2$, we construct inductively the sets A_m and B_m by the method explained in the proof of Theorem 1. We set $b_m := \#B_m$, $s_m := b_m/p$, and we choose the parameter T to be of the form

$$T := 2\lfloor \lambda \sqrt{p} \log p \rfloor + 1,$$

where $\lambda > 2$ is some parameter, for which we shall specify later an optimal value, and $\lfloor x \rfloor$ is the largest integer which is less than or equal to x. From the way the sets A_m and B_m are constructed for $m \geq 1$, it follows that as long as $s_m < 1/2$, A_{m+1} is obtained from A_m by adjoining to it just one element a_m of size no larger than T, and then B_{m+1} is taken to be $B_m \cup a_m \cdot B_m \pmod p$. Thus,

$$U_{m+1} := \sum_{x \in A_{m+1}} x \leq T + \sum_{x \in A_m} x = T + U_m, \quad \text{for } m \geq 1,$$

and therefore

$$U_{m+1} \leq mT + U_1, \tag{19}$$

and the above inequality (19) holds for all $m \geq 1$ as long as $s_m < 1/2$. However, by inequality (14) and our choice for T, it follows that when constructing A_{m+1} out of A_m, we choose the parameter M in such a way that

$$M < \frac{b_m^2}{p} + \frac{2b_m \sqrt{p} \log p}{T} < b_m \Big(s_m + \frac{1}{\lambda} \Big),$$

therefore inequality (17) now shows that

$$b_{m+1} \geq 2b_m - M > b_m \Big(\Big(2 - \frac{1}{\lambda} \Big) - s_m \Big).$$

Hence,

$$s_{m+1} > (\beta - s_m) s_m, \tag{20}$$

where

$$\beta := \beta(\lambda) := 2 - \frac{1}{\lambda} = \frac{2\lambda - 1}{\lambda}.$$

Of course, the above construction will be repeated only as long as $s_m < 1/2$. If we denote by n the largest positive integer such that $s_n < 1/2$, then $s_{n+1} \geq 1/2$, therefore the last set B_{n+2}, which is the entire $\mathbf{Z}_p^*$, is taken to be $B_{n+1} \cdot B_{n+1} \pmod p$, i.e., A_{n+2} is taken to be the list of elements A_{n+1}, but now each one of them is repeated twice. Thus,

$$U_{n+2} \leq 2U_{n+1} \leq 2(nT + U_1).$$

From these arguments, it follows that in order to insure that U_{n+2} is not larger than $p-1$, it suffices to check that

$$2(nT + U_1) < p. \tag{21}$$

The number U_1 can be easily computed in terms of A_1, therefore all we need in order to check that inequality (21) holds, is a good upper bound on n in terms of A_1. We recall that n is the largest positive integer with $s_n < 1/2$, where the sequence $(s_m)_{m\geq 1}$ has initial term $s_1 := b_1/p$ and satisfies the recurrence (20).

Step 2. We give an upper bound on n. Since $\lambda > 2$, it follows that $\beta > 3/2$, therefore inequality (20) shows that $s_{m+1} > s_m$ as long as $s_m < 1/2$. By (20), we also have

$$s_{k+1} > \beta s_k\Big(1 - \frac{s_k}{\beta}\Big), \qquad \text{for } k = 1,\ 2, \ldots,\ n,$$

therefore

$$s_{n+1} > \beta^n s_1 \prod_{k=1}^{n}\Big(1 - \frac{s_k}{\beta}\Big).$$

Since $s_k < 1/2$ for $k = 1,\ 2,\ \ldots,\ n$, it follows that

$$\frac{s_k}{\beta} < \frac{1}{2\beta} = \frac{\lambda}{2(2\lambda - 1)}.$$

The inequality

$$1 - x > e^{-\mu x} \tag{22}$$

holds for all x in the interval $\Big(0,\ \dfrac{\lambda}{2(2\lambda-1)}\Big)$ with some value $\mu := \mu(\lambda)$, and the best value of μ is precisely

$$\mu := -\frac{\log(1-x)}{x}\Big|_{x:=\frac{1}{2\beta}} = \frac{2(2\lambda-1)}{\lambda} \cdot \log\Big(\frac{4\lambda-2}{3\lambda-2}\Big). \tag{23}$$

The fact that the best value of μ for which inequality (22) holds with all x in the interval $\Big(0,\ \dfrac{1}{2\beta}\Big)$ is indeed the one given by formula (23) follows from the fact that the function $x \to -\dfrac{\log(1-x)}{x}$ is decreasing in the interval $\Big(0,\ \dfrac{1}{2\beta}\Big]$. Thus,

$$\log s_{n+1} > n\log\beta + \log s_1 + \sum_{k=1}^{n}\log\Big(1 - \frac{s_k}{\beta}\Big) > n\log\beta + \log s_1 - \frac{\mu}{\beta}\sum_{k=1}^{n} s_k. \tag{24}$$

We now find an upper bound on the sum appearing in the right hand side of inequality (24). Notice that since $\lambda > 1/2$, it follows that whenever $s_m < 1/2$, one also has

$$s_{m+1} > (\beta - s_m)s_m > (1+\rho)s_m,$$

where the best $\rho := \rho(\lambda)$ is given by

$$\beta - \frac{1}{2} = 1 + \rho,$$

or, equivalently,

$$\rho := \beta - \frac{3}{2} = \frac{1}{2} - \frac{1}{\lambda} = \frac{\lambda - 2}{2\lambda},$$

and

$$1+\rho=\frac{3\lambda-2}{2\lambda}.$$

In particular,

$$s_{n-1}<\frac{1}{1+\rho}s_n$$

holds, and if k is any positive integer less than n, then

$$s_{n-k}<\Big(\frac{1}{1+\rho}\Big)^k s_n$$

holds. Thus,

$$\sum_{k=1}^{n} s_k < s_n\sum_{k\geq 0}\Big(\frac{1}{1+\rho}\Big)^k < \frac{1}{2}\frac{\rho+1}{\rho}=\frac{3\lambda-2}{2(\lambda-2)}.$$

The above calculations show that

$$\log s_{n+1}>n\log\beta+\log s_1-\mu\cdot\frac{(3\lambda-2)\lambda}{2(2\lambda-1)(\lambda-2)}=n\log\beta+\log s_1-\gamma,$$

where

$$\gamma:=\gamma(\lambda):=\mu\cdot\frac{(3\lambda-2)\lambda}{2(2\lambda-1)(\lambda-2)}=\frac{(3\lambda-2)}{(\lambda-2)}\cdot\log\Big(\frac{4\lambda-2}{3\lambda-2}\Big).$$

Thus, if we choose n such that

$$n\log\beta+\log s_1-\gamma\geq\log(1/2), \tag{25}$$

then we are sure that $s_{n+1}>1/2$. Inequality (25) is equivalent to

$$n\log\beta>-\log(2s_1)+\gamma,$$

hence, to

$$n>\frac{1}{\log\beta}\Big(-\log(2s_1)+\gamma\Big).$$

Thus, we may write

$$n_0:=1+\Big\lfloor\frac{1}{\log\beta}\Big(-\log(2s_1)+\gamma\Big)\Big\rfloor, \tag{26}$$

and conclude that $n\leq n_0$. Thus, inequality (21) will be satisfied provided that

$$n_0T+U_1<\frac{p}{2} \tag{27}$$

holds, where n_0 is given by formula (26).

Step 3. Here, we show that we can do the above construction for $p>9\cdot 10^6$. From here on, we write $x:=p$ and $y:=\sqrt{\frac{x}{2}}$, and we assume that $x>2\cdot 10^6$. In particular, $y>10^3$. We choose

$$A_1:=\{q\mid q\text{ is prime and }q\leq y\},$$

and therefore

$$B_1 := \left\{ \frac{q_1}{2} \cdot \frac{q_2}{2} \;\middle|\; q_1 < q_2 \text{ and } q_1,\ q_2 \in A \right\}.$$

It is clear that the elements of B_1 are in distinct congruence classes in $\mathbf{Z}_p^*$, therefore we may consider B_1 as a subset of $\mathbf{Z}_p^*$ and its cardinality is precisely

$$b_1 := \binom{\pi(y)}{2} = \frac{\pi(y)(\pi(y)-1)}{2},$$

where $\pi(y)$ is the number of primes up to y. Thus,

$$\frac{1}{2s_1} = \frac{x}{\pi(y)(\pi(y)-1)}. \tag{28}$$

We next give an upper bound on U_1. We claim that

$$U_1 < \frac{1}{2} \cdot \pi(y)(\pi(y)+1)\Big(\log \pi(y) + \log\log \pi(y) - 1 + 1.8 \cdot \frac{\log\log \pi(y)}{\log \pi(y)}\Big). \tag{29}$$

The above formula follows almost immediately from inequality (v) from Théorème A in [4] which claims that

$$p_m < m\left(\log m + \log\log m - 1 + \frac{1.8 \log\log m}{\log m}\right), \qquad \text{holds for all } m \geq 13. \tag{30}$$

Here p_m denotes the mth prime number. The function

$$t \longmapsto \log t + \log\log t - 1 + 1.8 \cdot \frac{\log\log t}{\log t} \tag{31}$$

is increasing for $t > 13$. Moreover, since $y > 10^3$, it follows that $N := \pi(y) \geq 168$,

$$\log N + \log\log N - 1 + 1.8 \cdot \frac{\log\log N}{\log N} \geq \log 168 + \log\log 168 - 1 + 1.8 \cdot \frac{\log\log 168}{\log 168} \approx 6.33 > 6, \tag{32}$$

and

$$p_m < 6m \qquad \text{holds for } m = 1,\ 2,\ \ldots,\ 13. \tag{33}$$

The combination of (30)–(33) shows that

$$U_1 = \sum_{p \leq y} p < \Big(\log \pi(y) + \log\log \pi(y) - 1 + 1.8 \cdot \frac{\log\log \pi(y)}{\log \pi(y)}\Big) \cdot \sum_{k=1}^{N} k =$$

$$\frac{1}{2} \cdot N(N+1)\Big(\log \pi(y) + \log\log \pi(y) - 1 + 1.8 \cdot \frac{\log\log \pi(y)}{\log \pi(y)}\Big),$$

which is precisely inequality (29). Having expressed s_1 in terms of $\pi(y)$ and having found an upper bound for U_1 in terms of $\pi(y)$, we now use the fact that the inequalities

$$\frac{t}{\log t - 0.5} < \pi(t) < \frac{t}{\log t - 1.5}, \qquad \text{hold for all } t > 67 \tag{34}$$

(see Theorem 2 in [6]). We used the lower bounds for $\pi(y)$ given by inequality (34) in the formulae (28) and (26) in order to get an upper bound for n_0 in terms of x, as well as the upper bound for $\pi(y)$ given by the same inequality (34) in order to get an upper bound for U_1 in terms of x, inserted both of these into (27) and we got an inequality which is satisfied for all $x > 11 \cdot 10^6$ at $\lambda = 3$. Here, we used Mathematica[1] to check the resulting inequality (27). In fact, the resulting inequality was found to be true for all $x > 10.3 \cdot 10^6$ (but it fails at $x = 10.2 \cdot 10^6$). Finally, we checked, using again Mathematica, that (27) is true at $\lambda = 3$ for any prime number $x := p$ in the interval $(9 \cdot 10^6, 11 \cdot 10^6)$. In fact, the largest prime number $x := p$ for which (27) does not hold at $\lambda = 3$ is $p = 8269189$.

Step 4. It suffices to check that for all prime numbers $5 < p < 9 \cdot 10^6$, the set

$$\{\prod_{i=1}^{t} m_i! \mid \sum_{i=1}^{t} m_i = p - 1\} \tag{35}$$

covers the entire $\mathbf{Z}_p^*$. Here is a trick that worked for the primes p which are large enough.

Lemma 2.
Assume that $a > 1$ is a primitive root modulo p and assume that v and b are positive integers in the interval $(1,\ p-1)$ such that $b \equiv a^v \pmod{p}$ and

$$v^2 a < p(v - b). \tag{36}$$

Then, the set given by (35) covers $\mathbf{Z}_p^*$.

Proof. Take $w := \lfloor (p-1)/v \rfloor$, $t := (v-1) + w$, and $m_i := a$ for $i = 1,\ 2,\ \ldots,\ v-1$, and $m_i := b$ for $i = v,\ v+1,\ \ldots,\ t$. Notice first that

$$\sum_{i=1}^{t} m_i = (v-1)a + wb < va + \frac{p}{v} b < p,$$

where the last inequality from the right above follows from (36). Thus, we may complete the t-tuple $(m_1,\ \ldots,\ m_t)$ with ones until we get a longer vector whose sum of the coordinates is equal to $p-1$. Notice also that for each pair of nonnegative integers $(\lambda,\ \mu)$ with $\lambda \le v-1$ and $\mu \le w$ we have

$$(a!)^{v-1}(b!)^w = a^\lambda b^\mu \big((a-1)!^\lambda (b-1)!^\mu a!^r b!^s\big),$$

where $r = v - 1 - \lambda$ and $s = w - \mu$. Thus, it suffices to show that every congruence class in $\mathbf{Z}_p^*$ can be represented under the form $a^\lambda b^\mu$ for some nonnegative λ and μ with $\lambda \le v-1$ and $\mu \le w$. But clearly, every congruence class in $\mathbf{Z}_p^*$ is of the form a^t for some t in the interval $[1,\ p-1]$ because a is a primitive root modulo p. We may now apply the division with remainder theorem to write

$$t = \mu v + \lambda,$$

where $\lambda \le v-1$, and $\mu := \lfloor t/v \rfloor$. Thus, $\mu \le w$, and

$$a^t = a^{\mu v + \lambda} = a^\lambda (a^v)^\mu = a^\lambda b^\mu,$$

[1] A Trademark of Wolfram Research

and the lemma is therefore proved.

Before proceeding further into the final stages of the proof of our Theorem 2, one may ask whether or not for every sufficiently large prime number p there exist positive integers $a,\ b$, and v satisfying the hypothesis of Lemma 2. We have been unable to find an unconditional proof of such a statement, but it can be shown that this is indeed so under the Extended Riemann Hypothesis.

Lemma 3.
Assuming the Extended Riemann Hypothesis, there exists a constant p_0 so that if $p > p_0$ is a prime number then there exists integers $a,\ b,\ v$ in the interval $(1,\ p-1)$ with a a primitive root modulo p, $b \equiv a^v \pmod p$ and

$$v^2 a < p(v-b). \tag{37}$$

Proof. The following proof is due to Igor Shparlinski. Let p be a sufficiently large prime and let $H,\ K,\ M,\ N$ be positive numbers smaller than p. Let a be an arbitrary primitive root modulo p. It is then known, that the number of numbers $v \in [H,\ H+K]$ such that $a^v \pmod p \in [M+1,\ M+N]$ is $KN/p + O(p^{1/2}\log^2 p)$, where the constant understood in the above O is absolute (see [5]). We take $H := 2p^{3/4}\log^{5/4} p$, $K := 2p^{3/4}\log^{5/4} p$, $M := 1$ and $N := p^{3/4}\log^{5/4} p$. Thus, if a is any primitive root modulo p, then the number of numbers $v \in [2p^{3/4}\log^{5/4} p,\ 4p^{3/4}\log^{5/4} p]$ for which $a^v \pmod p \in [1,\ p^{3/4}\log^{5/4} p]$ is

$$\frac{KN}{p} + O(p^{1/2}\log^2 p) = p^{1/2}\log^{5/2} p + O(p^{1/2}\log^2 p) > 0$$

for p sufficiently large. Thus, if p is large and a is fixed, then there exists an integer v in the interval $[2p^{3/4}\log^{5/4} p,\ 4p^{3/4}\log^{5/4} p]$ so that if $b \equiv a^v \pmod p$, then $b \in [1,\ p^{3/4}\log^{5/4} p]$. This is so for an arbitrary primitive root a modulo p. Under the Extended Riemann Hypothesis, it is known (see [8] and [10]) that the smallest primitive root modulo p, let us call it $g(p)$, satisfies $g(p) = O(\omega(p-1)^6\log^2 p)$ where we use $\omega(p-1)$ for the number of distinct prime divisors of $p-1$. Since $\omega(p-1) = o(\log p)$, it follows that if p is large, then the interval $[1,\ \log^8 p]$ contains a primitive root a modulo p. In fact, for our argument it suffices that the interval $[1,\ p^{1/4}/\log^2 p]$ contains a primitive root a modulo p. With these choices of $a := g(p)$ and v, we have

$$av^2 \le \frac{p^{1/4}}{\log^2 p} \cdot (4p^{3/4}\log^{5/4} p)^2 = 16p^{7/4}\log^{1/2} p, \tag{38}$$

while

$$p(v-b) \ge \frac{pv}{2} \ge p^{7/4}\log^{5/4} p, \tag{39}$$

and now the combination of (38) and (39) obviously shows that (37) holds with these choices of a and v when p is large.

It could be that Hildebrand's improvements from [3] on Burgess's character sums estimates from [1] could lead to the conclusion that for large p the inequality $g(p) \le p^{1/4}/\log^2 p$ does indeed hold, and if this were so then our Lemma 3 will be true unconditionally. We have been unable to decide this question.

Step 5. We now return to the proof of the Theorem 2 and explain how we did the computations for the remaining primes $p < 9 \cdot 10^6$. We first showed computationally that for every prime number p in the interval $[7.6 \cdot 10^3,\ 9 \cdot 10^6]$ there exist integers $a,\ b$, and v satisfying the hypothesis of Lemma 2. For this, we fixed such a prime p. We took the first 25 odd primes and we checked each one of them against being a primitive root modulo p. It is clear that at least one of these numbers will be a primitive root modulo p for most of the primes p in our range. We collected all these primes which are primitive roots modulo p in a set which we called $A(p)$. Now we tried to find a value for v. We could have looped over all possible values of v, but this would have resulted in a cycle of length $p-1$ for each p, and the computation would have taken too long. Instead, let v_0 be an initial value of v and set $b \equiv a^{v_0} \pmod p$. If v_0 is good, we are done. If not, we set the next v to be such that

$$v := v_0 + 1 + \left\lfloor \frac{\log p/b}{\log a} \right\rfloor.$$

In a sense, the v shown above is the smallest $v > v_0$ one can choose for which there is a chance for $a^v = a^{v_0}a^{v-v_0} = ba^{v-v_0}$ to be small modulo p. We kept on doing this for about $3\sqrt{p}$ times for each $a \in A$. If no good values of a and v were found by this code, then we had the program put p in a list of "bad" primes. The computation was done with $v_0 := \lfloor \log p/\log a \rfloor$, but a different choice of v_0 might have given better results.
Now, $\pi(9 \cdot 10^6) = 602489 < 6.1 \cdot 10^5$. After the first run of the algorithm between the 100^{th} and 610000^{th} prime, we obtained a list of 1799 "bad" primes, the largest one of which being 9112771.
In the second iteration, we increased the range for v to $40\sqrt{p}$ and the range of odd primes which may be primitive roots modulo p to 80, and we sieved the previous list. The list shortened to 27 "bad" primes, the first one being 541 and the largest one being 7591. These primes were handled by a different method: we wrote a Mathematica program which showed that the union of the sets

$$A_p(s) = \left\{ 2^u \left(\frac{p-2s-1}{2} \right)! \,|\, 0 \le u \le \left\lfloor \frac{p+2s+1}{4} \right\rfloor \right\}, \tag{40}$$

where $0 \le s \le \frac{p-3}{2}$, covers the entire $\mathbf{Z}_p^*$, for any p in the remaining set of "bad" primes. In fact, the above sets were shown to cover Z_p^* for all the primes up to 1000 as well, except for $p = 5$. We conjecture that the union of (40) for all the possible values of s covers Z_p^* for any prime $p \neq 5$, but we have no idea of how to attack this question.

Acknowledgements. We thank Professors W.O. Nowell and Y. Song for their help with the programming in C++ which double-checked our computations done by Mathematica, and Professor Igor Shparlinski for various useful suggestions as well as for supplying the proof of Lemma 3. We also thank the anonymous referee for suggestions which improved the quality of this paper and for pointing out some errors in a previous version of this paper. The first author was supported in part by grants ECOS-ANUIES M02-M01, SEP-CONACYT 37259-E and SEP-CONACYT 37260-E. The second author was partially supported by a research grant from the School of Sciences at his institution.

References

[1] D.A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. **12** (1962), 179–192.

[2] C. Cobeli, M. Vâjâitu, A. Zaharescu, *The sequence* $n!$ (mod p), J. Ramanujan Math. Soc. **15** (2) (2000), 135-154.

[3] A. Hildebrand, *A note on Burgess' character sum estimate*, C. R. Math. Rep. Acad. Sci. Canada **8** (1) (1986), 35–37.

[4] J. Massias, G. Robin, *Bornes effectives pour certaines fonctions concernant les nombres premiers*, J. Théorie Nombres Bordeaux **8** (1996), 215-242.

[5] H.L. Montgomery, *Distribution of small powers of a primitive root,* in "Advances in number theory" (Kingston, ON, 1991), 137–149, Oxford Univ. Press, 1993.

[6] A. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64-94.

[7] A. Sárkőzy, *On the distribution of residues of products of integers*, Acta Math. Hung. **49** (3-4) (1987), 397-401.

[8] V. Shoup, *Searching for primitive roots in finite fields,* Math. Comp. **58** (1992), no. 197, 369–380.

[9] P. Stănică, p^q*-Catalan Numbers and Squarefree Binomial Coefficients*, to appear in Journal of Number Theory.

[10] Y. Wang, *On the least primitive root of a prime*, Acta Math. Sinica **10** (1961), 1–14.