PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 139, Number 5, May 2011, Pages 1569–1577
S 0002-9939(2010)10587-7
Article electronically published on October 28, 2010

BINOMIAL COEFFICIENTS AND THE RING OF p-ADIC INTEGERS

ZHI-WEI SUN AND WEI ZHANG

(Communicated by Wen-Ching Winnie Li)

Abstract. Let $k > 1$ be an integer and let p be a prime. We show that if $p^a \leqslant k < 2p^a$ or $k = p^a q + 1$ (with $q < p/2$) for some $a = 1, 2, 3, \ldots$, then the set $\{\binom{n}{k} : n = 0, 1, 2, \ldots\}$ is dense in the ring $\mathbb{Z}_p$ of p-adic integers; i.e., it contains a complete system of residues modulo any power of p.

1. Introduction

Let p be an odd prime. In section F11 of Guy [Gu, p. 381] it is conjectured that $|\{n! \bmod p : \ n = 1, 2, 3, \ldots\}|$ is about $p(1 - 1/e)$ asympototically. [CVZ] provided certain evidence for the conjecture.

In [BLSS] the authors proved that for infinitely many primes p there are at least $\log\log p/\log\log\log p$ distinct integers among $0, 1, \ldots, p-1$ which are not congruent to $n!$ for any $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.

Garaev and Luca [GL] showed that for any $\varepsilon > 0$ there is a computable positive constant $p_0(\varepsilon)$ such that for any prime $p > p_0(\varepsilon)$ and integers $t > p^\varepsilon$ and $s > t + p^{1/4+\varepsilon}$ we have

$$\{m_1! \cdots m_t! \ (\mathrm{mod}\, p) : \ m_1 + \cdots + m_t = s\} \supseteq \{r \ (\mathrm{mod}\ p) : \ r = 1, \ldots, p-1\}.$$

Let p be any prime. As usual, we denote by $\mathbb{Z}_p$ the ring of p-adic integers in the p-adic field $\mathbb{Q}_p$. The reader may consult an excellent book [M] by Murty for the basic knowledge of p-adic analysis. Any given p-adic integer α has a unique representation in the form

$$\alpha = \sum_{j=0}^{\infty} a_j p^j \quad \text{with } a_j \in [0, p-1] = \{0, 1, \ldots, p-1\}.$$

For each $b \in \mathbb{N} = \{0, 1, 2, \ldots\}$ we have

$$\alpha \equiv r(b) \ (\mathrm{mod}\, p^b), \quad \text{i.e.,} \quad |\alpha - r(b)|_p \leqslant \frac{1}{p^b},$$

where $r(b) := \sum_{0 \leqslant j < b} a_j p^j$ and $|\cdot|_p$ is the p-adic norm.

In this paper we study the following new problem (which was actually motivated by the first author's paper [S]).

Received by the editors December 26, 2009 and, in revised form, May 15, 2010.
2010 *Mathematics Subject Classification.* Primary 11B65; Secondary 05A10, 11A07, 11S99.
The first author is the corresponding author. He is supported by the National Natural Science Foundation (grant 10871087) and the Overseas Cooperation Fund (grant 10928101) of China.

Problem 1.1. Given a prime p and a positive integer k, is the set $\{\binom{n}{k}:\ n\in\mathbb{N}\}$ dense in $\mathbb{Z}_p$? In other words, does the set contain a complete system of residues modulo any power of p?

Definition 1.1. Let $k\in\mathbb{N}$ and $m\in\mathbb{Z}^+$, and define

$$R_m(k):=\left\{\binom{n}{k}\pmod m:\ n\in\mathbb{N}\right\}. \tag{1.1}$$

If $R_m(k)=\mathbb{Z}/m\mathbb{Z}$, then we call m a *k-universal* number.

Clearly all positive integers are 1-universal and 1 is k-universal for all $k\in\mathbb{Z}^+$.

If p is a prime, $a,k,n,n'\in\mathbb{N}$ and $n'\equiv n\pmod{p^{a+\mathrm{ord}_p(k!)}}$, then

$$\binom{n'}{k}=\frac{\prod_{0\leqslant j<k}(n'-j)}{k!}\equiv\frac{\prod_{0\leqslant j<k}(n-j)}{k!}=\binom{n}{k}\pmod{p^a}.$$

Combining this observation with the Chinese Remainder Theorem we immediately get the following basic proposition.

Proposition 1.1. *Let $k\in\mathbb{Z}^+$ and $m=p_1^{a_1}\cdots p_r^{a_r}$, where $p_1,\ldots,p_r$ are distinct primes and $a_1,\ldots,a_r\in\mathbb{Z}^+$. Then m is k-universal if and only if $p_1^{a_1},\ldots,p_r^{a_r}$ are all k-universal.*

In view of Proposition 1.1, we may focus on those k-universal prime powers.

Let $k>1$ be an integer. If $p>k$ is a prime, then p is not k-universal since

$$\left\{\binom{0}{k},\binom{1}{k},\ldots,\binom{p-1}{k}\right\}$$

is not a complete system of residues modulo p. (Note that $\binom{0}{k}=\binom{1}{k}=0$.) Thus, if $m\in\mathbb{Z}^+$ is k-universal, then m has no prime divisor greater than k.

For an integer $k>1$, a prime $p>k$ and an integer $r\in[1,p-1]=\{1,\ldots,p-1\}$, the congruence $\binom{x}{k}\equiv r\pmod p$ might have more than two solutions. For example,

$$\binom{12}{5}\equiv\binom{19}{5}\equiv\binom{22}{5}\equiv\binom{31}{5}\equiv 18\pmod{43}$$

and

$$\binom{15}{10}\equiv\binom{21}{10}\equiv\binom{25}{10}\equiv\binom{30}{10}\equiv 14\pmod{61}.$$

Recall the following useful result of Lucas.

Lucas' Theorem (cf. [Gr] and [HS]). *Let p be any prime, and let $n_0,k_0,\ldots,n_r,k_r\in[0,p-1]$. Then we have*

$$\binom{\sum_{i=0}^r n_ip^i}{\sum_{i=0}^r k_ip^i}\equiv\prod_{i=0}^r\binom{n_i}{k_i}\pmod p.$$

Clearly Lucas' theorem implies the following proposition.

Proposition 1.2. *Let p be a prime and let $k=\sum_{i=0}^r k_ip^i$ with $k_i\in[0,p-1]$. Then $R_p(k)=\prod_{i=1}^r R_p(k_i)$. In particular, when $k_0,\ldots,k_r\in\{0,p-2,p-1\}$ we have*

$$R_p(k)\subseteq\{r\pmod p:\ r=0,\pm1\}.$$

Let p be a prime. As $R_p(1) = \mathbb{Z}/p\mathbb{Z}$, if the p-adic expansion of $k \in \mathbb{Z}^+$ has a digit 1, then $R_p(k) = \mathbb{Z}/p\mathbb{Z}$ by Proposition 1.2. In this spirit, Proposition 1.2 is helpful to study when $R_p(k) = \mathbb{Z}/p\mathbb{Z}$. For an integer $b > 1$, to investigate whether p^b is k-universal (i.e., $R_{p^b}(k) = \mathbb{Z}/p^b\mathbb{Z}$) one might think that we should use an extended Lucas theorem for prime powers. However, all known generalizations of Lucas' theorem to prime powers are somewhat unnatural and complicated, e.g., Davis and Webb [DW] proved that if $p > 3$ is a prime, $a, b, n, k \in \mathbb{Z}^+$ and $n_0, k_0 \in [0, p^a - 1]$, then

$$\binom{np^{a+b} + n_0}{kp^{a+b} + k_0} \equiv \binom{np^{\lfloor b/3 \rfloor}}{kp^{\lfloor b/3 \rfloor}} \binom{n_0}{k_0} \pmod{p^{b+1}}.$$

Therefore, we prefer to approach Problem 1.1 by an induction argument which can be easily understood.

Our first result is as follows.

Theorem 1.1. *Let p be a prime and let $a \in \mathbb{N} = \{0, 1, 2, \ldots\}$. Let k be an integer with $p^a \leqslant k < 2p^a$. Then, for any $b \in \mathbb{N}$ and $r \in \mathbb{Z}$ there is an integer $n \in [0, p^{a+b} - 1]$ with $n \equiv k \pmod{p^a}$ such that $\binom{n}{k} \equiv r \pmod{p^b}$.*

Remark 1.1. For a prime p and a positive integer k having a digit 1 in its p-adic expansion, p is definitely k-universal (i.e., $R_p(k) = \mathbb{Z}/p\mathbb{Z}$) but p^b might not be for some integer $b > 1$. For example, $21 = 4 \times 5 + 1$ and $\mathrm{ord}_5(21!) = 4$. Thus

$$\begin{aligned}\left\{\binom{n}{21} \pmod{5^2} :\ n \in \mathbb{N}\right\} &= \left\{\binom{n}{21} \pmod{5^2} :\ n \in [0, 5^6 - 1]\right\} \\ &= \{r \pmod{5^2} :\ r = 0, \pm 1, \pm 3, \pm 5, \pm 10\},\end{aligned}$$

and hence $R_{5^2}(21) \neq \mathbb{Z}/5^2\mathbb{Z}$.

Here is a consequence of Theorem 1.1.

Corollary 1.1. *Let p be a prime and let $k \in \mathbb{Z}^+$ with $\log_p(k/2) < \lfloor \log_p k \rfloor$. Then $1, p, p^2, \ldots$ are k-universal numbers, and the set $\{\binom{n}{k} : n \in \mathbb{N}\}$ is a dense subset of the ring $\mathbb{Z}_p$ of p-adic integers.*

Proof. Set $a = \lfloor \log_p k \rfloor$. Then $p^a \leqslant k < 2p^a$. By Theorem 1.1, p^b is k-universal for every $b = 0, 1, 2, \ldots$. Therefore $\{\binom{n}{k} : n \in \mathbb{N}\}$ is dense in $\mathbb{Z}_p$. This concludes the proof. □

For any $k \in \mathbb{Z}^+$ there is a unique $a \in \mathbb{N}$ such that $2^a \leqslant k < 2^{a+1}$. Thus Theorem 1.1 or Corollary 1.1 implies the following result.

Corollary 1.2. *Let $k \in \mathbb{Z}^+$. Then any power of two is k-universal, and hence the set $\{\binom{n}{k} : n \in \mathbb{N}\}$ is a dense subset of the 2-adic integral ring $\mathbb{Z}_2$.*

Definition 1.2. A positive integer k is said to be *universal* if any power of a prime $p \leqslant k$ is k-universal, i.e., $\{\binom{n}{k} : n \in \mathbb{N}\}$ is a dense subset of $\mathbb{Z}_p$ for any prime $p \leqslant k$.

Theorem 1.1 implies that 1, 2, 3, 4, 5, and 9 are universal numbers. To obtain other universal numbers, we need to extend Theorem 1.1.

Theorem 1.2. *Let p be a prime and let $a \in \mathbb{N}$. Let $k = k_0 + p^a k_1$ with $k_0 \in [0, p^a - 1]$ and $k_1 \in [1, p - 1]$. Suppose that for each $r = 1, \ldots, p - 1$ there are $n_0 \in [k_0, p^a - 1]$ and $n_1 \in [k_1, p - 1]$ such that*

$$\binom{n_1}{k_1}\binom{n_0}{k_0} \equiv r \pmod{p} \quad \text{and} \quad P_{k_1}(n_1) \not\equiv 0 \pmod{p}, \tag{1.2}$$

where

$$P_{k_1}(x)=\sum_{j=1}^{k_1}\frac{(-1)^{j-1}}{j}\binom{x}{k_1-j}. \tag{1.3}$$

Then, for any $b\in\mathbb{N}$, the set $\{\binom{n}{k}: n\in[0,p^{a+b}-1]\}$ contains a complete system of residues modulo p^b.

Remark 1.2. Let p be an odd prime. Then

$$\begin{aligned}P_{p-1}(p-1)&=\sum_{j=1}^{p-1}\frac{(-1)^{j-1}}{j}\binom{p-1}{j}\\&\equiv-\sum_{j=1}^{p-1}\frac{1}{j}=-\sum_{j=1}^{(p-1)/2}\left(\frac{1}{j}+\frac{1}{p-j}\right)\equiv 0\ (\mathrm{mod}\,p).\end{aligned}$$

Thus, for $k_1=p-1$ there is no $n_1\in[k_1,p-1]$ with $P_{k_1}(n_1)\not\equiv 0\ (\mathrm{mod}\,p)$.

Corollary 1.3. *Let p be an odd prime and $q\in\{1,\ldots,(p-1)/2\}$. Then, for any $a\in\mathbb{Z}^+$ and $b\in\mathbb{N}$, the number p^b is (p^aq+1)-universal.*

Proof. Let $k_1=q$, $k_0=1$, and $k=p^ak_1+k_0=p^aq+1$. As $P_{k_1}(x)\equiv 0\ (\mathrm{mod}\,p)$ cannot have more than $\deg P_{k_1}(x)=k_1-1$ solutions (see, e.g., [IR, p. 39]), there exists $n_1\in[k_1,2k_1-1]\subseteq[k_1,p-1]$ such that $P_{k_1}(n_1)\not\equiv 0\ (\mathrm{mod}\,p)$. Note that $\binom{n_1}{k_1}\not\equiv 0\ (\mathrm{mod}\,p)$. For any $r\in[1,p-1]$ there is a unique $n_0\in[1,p-1]$ such that

$$\binom{n_1}{k_1}\binom{n_0}{k_0}=n_0\binom{n_1}{k_1}\equiv r\ (\mathrm{mod}\,p).$$

Applying Theorem 1.2, we immediately obtain the desired result. □

From Theorem 1.2 we can deduce the following result.

Theorem 1.3. *The integers* 11, 17 *and* 29 *are universal numbers.*

We have the following conjecture based on our computation via the software `Mathematica`.

Conjecture 1.1. *There are no universal numbers other than* 1, 2, 3, 4, 5, 9, 11, 17, *and* 29.

In Sections 2, 3 and 4 we will prove Theorems 1.1, 1.2 and 1.3 respectively.

2. Proof of Theorem 1.1

We use induction on b. The case $b=0$ is trivial, so we proceed to the induction step.

Now fix $b\in\mathbb{N}$ and $r\in\mathbb{Z}$. Suppose that $m\in\mathbb{Z}$, $n=k+p^am\in[0,p^{a+b}-1]$ and $\binom{n}{k}\equiv r\ (\mathrm{mod}\,p^b)$. Let q be the smallest nonnegative residue of $(r-\binom{n}{k})/p^b$ modulo p.

Set $n'=n+p^{a+b}q$. Then

$$n'<p^{a+b}(q+1)\leqslant p^{a+b+1}\ \text{ and }\ n'\equiv n\equiv k\ (\mathrm{mod}\,p^a).$$

By the Chu-Vandermonde identity (cf. (5.22) of [GKP, p. 169]),

$$\binom{n'}{k}=\binom{n+p^{a+b}q}{k}=\sum_{j=0}^{k}\binom{p^{a+b}q}{j}\binom{n}{k-j}.$$

If $1 \leqslant j \leqslant k$ and $j \neq p^a$, then $p^a \nmid j$ and hence

$$\binom{p^{a+b}q}{j} = \frac{p^{a+b}q}{j}\binom{p^{a+b}q-1}{j-1} \equiv 0 \pmod{p^{b+1}}.$$

Note also that

$$\binom{p^{a+b}q}{p^a} = p^b q \prod_{t=1}^{p^a-1} \frac{p^{a+b}q-t}{t} \equiv p^b q(-1)^{p^a-1} \equiv p^b q \pmod{p^{b+1}}.$$

Therefore

$$\binom{n'}{k} \equiv \binom{n}{k} + p^b q\binom{n}{k-p^a} \equiv r - p^b q + p^b q\binom{n}{k-p^a} \pmod{p^{b+1}}.$$

So it suffices to show that

$$\binom{n}{k-p^a} \equiv 1 \pmod{p}.$$

As $0 \leqslant k-p^a < p^a$, Lucas' theorem implies that

$$\binom{n}{k-p^a} = \binom{(m+1)p^a + (k-p^a)}{0p^a + (k-p^a)} \equiv \binom{m+1}{0}\binom{k-p^a}{k-p^a} = 1 \pmod{p}.$$

Combining the above we have completed the proof by induction.

3. Proof of Theorem 1.2

We claim that for each $b = 0, 1, 2, \ldots$ the set $\{\binom{n}{k} : n \in S(b)\}$ contains a complete system of residues modulo p^b, where

$$S(b) = \left\{n \in [0, p^{a+b}-1] : \binom{\{n\}_{p^a}}{k_0}\sum_{j=1}^{k_1}\frac{(-1)^{j-1}}{j}\binom{\lfloor n/p^a\rfloor}{k_1-j} \not\equiv 0 \pmod{p}\right\}$$

and $\{n\}_{p^a}$ denotes the least nonnegative residue of n mod p^a.

The claim is trivial for $b = 0$ since

$$\binom{\{k_0\}_{p^a}}{k_0}\sum_{j=1}^{k_1}\frac{(-1)^{j-1}}{j}\binom{\lfloor k_0/p^a\rfloor}{k_1-j} = \frac{(-1)^{k_1-1}}{k_1} \not\equiv 0 \pmod{p}.$$

As $\deg P_{k_1}(x) < k_1$, there exists $n_1 \in [0, k_1-1]$ such that $P_{k_1}(n_1) \not\equiv 0 \pmod{p}$. Combining this with the supposition in Theorem 1.2, we see that for any $r \in [0, p-1]$ there are $n_0 \in [0, p^a-1]$ and $n_1 \in [0, p-1]$ satisfying (1.2) and the congruence $\binom{n_0}{k_0} \not\equiv 0 \pmod{p}$. Taking $n = p^a n_1 + n_0 \in [0, p^{a+1}-1]$ we find that

$$\binom{n}{k} \equiv \binom{n_1}{k_1}\binom{n_0}{k_0} \equiv r \pmod{p}$$

by Lucas' theorem. This proves the claim for $b = 1$.

Now let $b \in \mathbb{Z}^+$ and assume that $\{\binom{n}{k} : n \in S(b)\}$ contains a complete system of residues modulo p^b. We proceed to prove the claim for $b+1$.

Let r be any integer. By the induction hypothesis, there is an integer $n \in [0, p^{a+b}-1]$ such that

$$\binom{n}{k} \equiv r \pmod{p^b} \quad \text{and} \quad \binom{n_0}{k_0}\sum_{j=1}^{k_1}\frac{(-1)^{j-1}}{j}\binom{\lfloor n/p^a\rfloor}{k_1-j} \not\equiv 0 \pmod{p},$$

where $n_0=\{n\}_{p^a}$. Hence, for some $q\in[0,p-1]$ we have

$$q\binom{n_0}{k_0}\sum_{j=1}^{k_1}\frac{(-1)^{j-1}}{j}\binom{\lfloor n/p^a\rfloor}{k_1-j}\equiv\frac{r-\binom{n}{k}}{p^b}\pmod p.$$

Clearly, $n'=n+p^{a+b}q\in[0,p^{a+b+1}-1]$ and

$$\begin{aligned}&\binom{\{n'\}_{p^a}}{k_0}\sum_{j=1}^{k_1}\frac{(-1)^{j-1}}{j}\binom{\lfloor n'/p^a\rfloor}{k_1-j}\\=&\binom{n_0}{k_0}\sum_{j=1}^{k_1}\frac{(-1)^{j-1}}{j}\binom{\lfloor n/p^a\rfloor+p^bq}{k_1-j}\\\equiv&\binom{n_0}{k_0}\sum_{j=1}^{k_1}\frac{(-1)^{j-1}}{j}\binom{\lfloor n/p^a\rfloor}{k_1-j}\not\equiv 0\pmod p.\end{aligned}$$

As in the proof of Theorem 1.1, we have

$$\begin{aligned}\binom{n'}{k}-\binom{n}{k}=&\sum_{j=1}^{k}\binom{p^{a+b}q}{j}\binom{n}{k-j}\\\equiv&\sum_{j=1}^{\lfloor k/p^a\rfloor}\binom{p^{a+b}q}{p^aj}\binom{n}{k-p^aj}\pmod{p^{b+1}}.\end{aligned}$$

By Lucas' theorem, for $1\leqslant j\leqslant\lfloor k/p^a\rfloor=k_1$ we have

$$\binom{p^{a+b}q}{p^aj}\equiv\binom{p^bq}{j}=\frac{p^bq}{j}\prod_{0<i<j}\frac{p^bq-i}{i}\equiv p^bq\frac{(-1)^{j-1}}{j}\pmod{p^{b+1}}$$

and

$$\binom{n}{k-p^aj}=\binom{p^a\lfloor n/p^a\rfloor+n_0}{p^a(k_1-j)+k_0}\equiv\binom{\lfloor n/p^a\rfloor}{k_1-j}\binom{n_0}{k_0}\pmod p.$$

Therefore

$$\binom{n'}{k}-\binom{n}{k}\equiv p^bq\binom{n_0}{k_0}\sum_{j=1}^{k_1}\frac{(-1)^{j-1}}{j}\binom{\lfloor n/p^a\rfloor}{k_1-j}\equiv r-\binom{n}{k}\pmod{p^{b+1}},$$

and hence $\binom{n'}{k}\equiv r\pmod{p^{b+1}}$. This concludes the induction step.

In view of the above we have proved the claim, and hence the desired result follows.

4. Proof of Theorem 1.3

(I) We first prove that 11 is universal.

Since

$$2^3<11<2^4,\ \ 3^2<11<2\times3^2,\ \ 7<11<2\times7,$$

and $11=2\times5+1$ with $2\leqslant(5-1)/2$, by Theorem 1.1 and Corollary 1.3, 11 is universal.

(II) Now we want to show that 17 is universal.

Observe that

$$2^4<17<2^5,\ \ 3^2<17<2\times3^2,\ \ 11<17<2\times11,$$

and $13 < 17 < 3 \times 13$. By Theorem 1.1, p^b is 17-universal for any $p = 2, 3, 11, 13$ and $b \in \mathbb{N}$.

Note that

$$\sum_{j=1}^{\lfloor 17/5 \rfloor} \frac{(-1)^{j-1}}{j} \binom{x}{\lfloor 17/5 \rfloor - j} = \frac{x^2 - 2x}{2} + \frac{1}{3} \equiv \frac{(x-1)^2 - 2}{2} \not\equiv 0 \pmod 5.$$

Also, $17 = 3 \times 5 + 2$ and

$$\begin{aligned} &\binom{3}{3}\binom{2}{2} \equiv 1 \pmod 5, \quad \binom{3}{3}\binom{3}{2} \equiv 3 \pmod 5, \\ &\binom{4}{3}\binom{2}{2} \equiv 4 \pmod 5, \quad \binom{4}{3}\binom{3}{2} \equiv 2 \pmod 5. \end{aligned}$$

So, by Theorem 1.2, 5^b is 17-universal for any $b \in \mathbb{N}$.

Clearly,

$$\sum_{j=1}^{\lfloor 17/7 \rfloor} \frac{(-1)^{j-1}}{j} \binom{x}{\lfloor 17/7 \rfloor - j} = x - \frac{1}{2} \equiv x - 4 \pmod 7.$$

Also, $17 = 2 \times 7 + 3$ and

$$\begin{aligned} &\binom{2}{2}\binom{3}{3} \equiv 1 \pmod 7, \quad \binom{2}{2}\binom{4}{3} \equiv 4 \pmod 7, \quad \binom{2}{2}\binom{5}{3} \equiv 3 \pmod 7, \\ &\binom{2}{2}\binom{6}{3} \equiv 6 \pmod 7, \quad \binom{3}{2}\binom{4}{3} \equiv 5 \pmod 7, \quad \binom{3}{2}\binom{5}{3} \equiv 2 \pmod 7. \end{aligned}$$

Thus, 7^b is also 17-universal for any $b \in \mathbb{N}$.

(III) Finally, we prove that 29 is universal.

By Theorem 1.1, it remains to prove that p^b is 29-universal for any $p = 7, 11, 13$ and $b \in \mathbb{N}$.

Note that $29 = 4 \times 7 + 1$. It is easy to check that

$$\sum_{j=1}^{4} \frac{(-1)^{j-1}}{j} \binom{4}{4-j} \not\equiv 0 \pmod 7.$$

For any $r \in [1, 6]$, we have $\binom{4}{4}\binom{r}{1} \equiv r \pmod 7$. So, by Theorem 1.2, 7^b is 29-universal for any $b \in \mathbb{N}$.

Clearly $29 = 2 \times 11 + 7$ and

$$\sum_{j=1}^{2} \frac{(-1)^{j-1}}{j} \binom{x}{2-j} = x - \frac{1}{2} \equiv x - 6 \pmod{11}.$$

Observe that

$$\binom{2}{2}\binom{7}{7}\equiv 1\pmod{11},\ \binom{2}{2}\binom{8}{7}\equiv -3\pmod{11},$$
$$\binom{2}{2}\binom{9}{7}\equiv 3\pmod{11},\ \binom{2}{2}\binom{10}{7}\equiv -1\pmod{11},$$
$$\binom{3}{2}\binom{8}{7}\equiv 2\pmod{11},\ \binom{3}{2}\binom{9}{7}\equiv -2\pmod{11},$$
$$\binom{4}{2}\binom{7}{7}\equiv -5\pmod{11},\ \binom{4}{2}\binom{10}{7}\equiv 5\pmod{11},$$
$$\binom{4}{2}\binom{8}{7}\equiv 4\pmod{11},\ \binom{4}{2}\binom{9}{7}\equiv -4\pmod{11}.$$

Applying Theorem 1.2 we see that 11^b is 29-universal for any $b\in\mathbb{N}$.

Observe that $29=2\times 13+3$ and

$$\sum_{j=1}^{2}\frac{(-1)^{j-1}}{j}\binom{x}{2-j}=x-\frac{1}{2}\equiv x-7\pmod{13}.$$

Also,

$$\binom{2}{2}\binom{3}{3}\equiv 1\pmod{13},\ \binom{2}{2}\binom{4}{3}\equiv 4\pmod{13},$$
$$\binom{2}{2}\binom{5}{3}\equiv -3\pmod{13},\ \binom{2}{2}\binom{6}{3}\equiv -6\pmod{13},$$
$$\binom{2}{2}\binom{7}{3}\equiv -4\pmod{13},\ \binom{2}{2}\binom{9}{3}\equiv 6\pmod{13},$$
$$\binom{2}{2}\binom{10}{3}\equiv 3\pmod{13},\ \binom{2}{2}\binom{12}{3}\equiv -1\pmod{13},$$
$$\binom{3}{2}\binom{6}{3}\equiv -5\pmod{13},\ \binom{3}{2}\binom{9}{3}\equiv 5\pmod{13},$$
$$\binom{4}{2}\binom{4}{3}\equiv -2\pmod{13},\ \binom{4}{2}\binom{7}{3}\equiv 2\pmod{13}.$$

Thus, with the help of Theorem 1.2, 13^b is 29-universal for any $b\in\mathbb{N}$.

By the above, we have completed the proof of Theorem 1.3.

Acknowledgment

The authors are grateful to the referee for many helpful comments.

References

[BLSS] W. D. Banks, F. Luca, I. E. Shparlinski and H. Stichtenoth, *On the value set of $n!$ modulo a prime*, Turk. J. Math. **29** (2005), 169–174. MR2142292 (2006b:11119)

[CVZ] C. Cobeli, M. Vajaitu and A. Zaharescu, *The sequence $n!\pmod p$*, J. Ramanujan Math. Soc. **15** (2000), 135–154. MR1754715 (2001g:11153)

[DW] K. Davis and W. Webb, *A binomial coefficient congruence modulo prime powers*, J. Number Theory **43** (1993), 20–23. MR1200804 (93m:11016)

[GL] M. Z. Garaev and F. Luca, *Character sums and products of factorials modulo p*, J. Théor. Nombres Bordeaux **17** (2005), 151–160. MR2152216 (2006b:11102)

[GKP] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, 2nd ed., Addison-Wesley, New York, 1994. MR1397498 (97d:68003)

[Gr] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, in: Organic Mathematics (Burnady, BC, 1995), 253–276, CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997. MR1483922 (99h:11016)

[Gu] R. K. Guy, *Unsolved Problems in Number Theory*, 2nd edition, Springer, New York, 1994. MR1299330 (96e:11002)

[HS] H. Hu and Z. W. Sun, *An extension of Lucas' theorem*, Proc. Amer. Math. Soc. **129** (2001), 3471–3478. MR1860478 (2002i:11019)

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Graduate Texts in Math., 84), 2nd ed., Springer, New York, 1990. MR1070716 (92e:11001)

[M] M. R. Murty, *Introduction to p-adic Analytic Number Theory* (AMS/IP Studies in Adv. Math., vol. 27), Amer. Math. Soc., Providence, RI; Internat. Press, Somerville, MA, 2002. MR1913413 (2003c:11151)

[S] Z. W. Sun, *On sums of primes and triangular numbers*, Journal of Combinatorics and Number Theory **1** (2009), 65–76.

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: zwsun@nju.edu.cn

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: zhangwei_07@yahoo.com.cn