THEOREM OF THE DAY

Wolstenholme's Theorem *If $p \geq 5$ is prime, then* $\binom{2p-1}{p-1} \equiv 1 \bmod p^3$.

1															
1	1														
1	2	1													
1	3	3	1												
1	4	6	4	1											
1	5	10	10	5	1										
1	6	15	20	15	6	1									
1	7	21	35	35	21	7	1								
1	8	28	56	70	56	28	8	1							
1	9	36	84	126	126	84	36	9	1						
1	10	45	120	210	252	210	120	45	10	1					
1	11	55	165	330	462	462	330	165	55	11	1				
1	12	66	220	495	792	924	792	495	220	66	12	1			
1	13	78	286	715	1287	1716	1716	1287	715	286	78	13	1		
1	14	91	364	1001	2002	3003	3432	3003	2002	1001	364	91	14	1	
1	15	105	455	1365	3003	5005	6435	6435	5005	3003	1365	455	105	15	1
1	16	120	560	1820	4368	8008	11440	12870	11440	8008	4368	1820	560	120	16
1	17	136	680	2380	6188	12376	19448	24310	24310	19448	12376	6188	2380	680	136
1	18	153	816	3060	8568	18564	31824	43758	48620	43758	31824	18564	8568	3060	816
1	19	171	969	3876	11628	27132	50388	75582	92378	92378	75582	50388	27132	11628	3876
1	20	190	1140	4845	15504	38760	77520	125970	167960	184756	167960	125970	77520	38760	15504
1	21	210	1330	5985	20349	54264	116280	203490	293930	352716	352716	293930	203490	116280	54264
1	22	231	1540	7315	26334	74613	170544	319770	497420	646646	705432	646646	497420	319770	170544
1	23	253	1771	8855	33649	100947	245157	490314	817190	1144066	1352078	1352078	1144066	817190	490314
1	24	276	2024	10626	42504	134596	346104	735471	1307504	1961256	2496144	2704156	2496144	1961256	1307504
1	25	300	2300	12650	53130	177100	480700	1081575	2042975	3268760	4457400	5200300	5200300	4457400	3268760
1	26	325	2600	14950	65780	230230	657800	1562275	3124550	5311735	7726160	9657700	10400600	9657700	7726160

The fact that p divides $\binom{2p-1}{p-1} - 1$ for any prime p can be deduced easily from the remarkable theorem of Lucas which says that $\binom{n}{k}$ is congruent, mod p, to the product $\prod \binom{n_i}{k_i}$, where the n_i and k_i are matching pairs of digits in the base-p representations of n and k. Indeed, $\binom{n}{k} \equiv \binom{pn}{pk}$ mod p, since multiplying by p merely contributes an extra zero to a base-p representation. Now take $n = 2$ and $k = 1$, giving $\binom{2}{1} \equiv \binom{2p}{p}$ mod p, or $2 \equiv 2\binom{2p-1}{p-1}$ mod p. Further investigation reveals that, for odd primes p, $\binom{n}{k} \equiv \binom{pn}{pk}$ mod p^2. And indeed we can advance to $\binom{n}{k} \equiv \binom{pn}{pk}$ mod p^3, for primes $p \geq 5$. For example, taking $n = 4$, $k = 3$ and $p = 5$ we can confirm that $4 = \binom{4}{3} \equiv \binom{20}{15} = 15504 \pmod{125}$ (the single, boxed figures, left).

But here it stops. E.g. $3 = \binom{3}{2} \not\equiv \binom{21}{14} = 116280 \pmod{7^4}$ (the circled figures). In fact, the least values p for which $\binom{2p-1}{p-1} \equiv 1$ mod p^4 holds are 16843 and 2124679 (the first two so-called *Wolstenholme primes*).

Moving deeper into number theory, let $H_{n,m}$ denote the sum $1 + 1/2^m + 1/3^m + \ldots + 1/n^m$. Then $\frac{1}{2}\left(H^2_{p-1,1} - H_{p-1,2}\right)$ is the coefficient of p^2 in the product $\left(1+\frac{p}{1}\right)\left(1+\frac{p}{2}\right)\cdots\left(1+\frac{p}{p-1}\right)$ and so $\binom{2p-1}{p-1} = \prod_{k=1}^{p-1}\left(1+\frac{p}{k}\right)$ is given mod p^3 by the sum $1 + pH_{p-1,1} + \frac{1}{2}p^2\left(H^2_{p-1,1} - H_{p-1,2}\right)$. Now, it may be established that $H_{p-1,1} \equiv 0$ mod p^2 (i.e. numerator of $H_{p-1,1}$ is divisible by p^2), and $H_{p-1,2} \equiv 0$ mod p. Substituting into our mod p^3 sum, taking a little care that the fractions behave as they should, this is enough to confirm that p^3 divides $\binom{2p-1}{p-1} - 1$.

Charles Babbage proved in 1819 that p^2 divides $\binom{2p-1}{p-1} - 1$. Joseph Wolstenholme's congruences, both the binomial and the more influential $H_{m,n}$ 'harmonic series' forms, date from 1862.

Weblink: arxiv.org/abs/1111.3057

Further reading: An Introduction to the Theory of Numbers by G.H. Hardy and E.W. Wright, OUP, 6th edition, 2008, chapter 7.