

Orders and Binomial Coefficients

Here I give some additional information on p -exponents of binomial coefficients and we discuss some further examples and applications of the notion of order modulo n . We start with binomial coefficients.

First we introduce some terminology. Let p be a prime number and n arbitrary. If $p^k \mid n$ but $p^{k+1} \nmid n$ then we say that k is the p -exponent of n . Concerning binomial coefficients I found the following useful and astonishing result due to Kummer:

Theorem 0.1. *Let m and n be positive integers and let p be a prime number. Write m and n in base p and perform the addition $m+n$ in base p . The number of carries in this addition is equal to the p -exponent of the binomial coefficient*

$$\binom{m+n}{m}.$$

As an example, let $n > m$ be two non-negative integers and let p be prime. We compute the p -exponent of $\binom{p^n}{p^m}$. We need to look at the addition $(p^n - p^m) + p^m = p^n$ in base p . In base p this reads

$$\underbrace{((p-1)(p-1)\dots(p-1)00\dots0)}_{n-m} + \underbrace{(100\dots0)}_m = \underbrace{100\dots0}_n.$$

Obviously a carry takes place precisely at the $n - m$ leftmost digits, so the p -exponent equals $n - m$.

As another application we will complete the second step in the proof of IMO 90 Nr 3, as discussed at the last meeting in Zurich. Because the obtained result is interesting in its own and has many applications besides this specific problem, we will do it a bit more generally. First we need a technical lemma, whose proof is a bit delicate due to the full generality of the result.

Lemma 0.2. *Let p be a prime and let n be a positive integer which is divisible by p^k , $k \geq 1$. Then the number*

$$\binom{n}{r} p^r$$

is divisible by p^{k+2} under the hypothesis that

- $2 \leq r \leq n$ if $p \geq 3$,
- $3 \leq r \leq n$ if $p = 2$.

Proof. we will prove that the involved binomial coefficient is divisible by p^{k+2-r} for $2 \leq r \leq k+2$ if $p \geq 3$ and for $3 \leq r \leq k+2$ if $p = 2$ (this is obviously enough because for $r > k+2$ the lemma is trivially true).

Assume that the p -exponent of r equals l . We claim that $l \leq k$. Consider the inequalities $p^l \leq r \leq k+2$. If $p \geq 3$ we have $k+2 \leq p^k$ for $k \geq 1$ and we are done. If $p = 2$ and $k \geq 2$ the same argument gives $k+2 \leq 2^k$. If $p = 2$ and $k = 1$ then $r = 3$ and the claim is trivial in this case.

We need to look at the addition $(n-r) + r = n$ in base p . Assume first that $l < k$. Then the p -exponent of both $n-r$ and r equals l . Now in base p this means that these two numbers

each end in l zeros, while n ends in k zeros. So addition of these numbers produces a carry at each of the positions $l+1, l+2, \dots, l$ counted from the right. According to the theorem, the p -exponent of $\binom{n}{r}$ is at least $k-l$. If $l=k$ then again we have that the p -exponent of the binomial coefficient is at least $0 = k-l$ from trivial reasons.

We are done if we can prove that $k-l \geq k+2-r$. This is equivalent to $r \geq l+2$. We distinguish some cases. If $l=0$ this is true in view of $r \geq 2$. If $l \geq 1$ and $p \geq 3$ then again $r \geq p^l \geq 3^l \geq l+2$ for $l \geq 1$. Now assume that $p=2$. If $l=1$ then this is true because $r \geq 3$. If $l \geq 2$ then again $r \geq 2^l \geq l+2$. we are done in all cases. □

Lets use this.

Lemma 0.3. *Let $p \geq 3$ be a prime number and let n be an odd integer. Assume that the p -exponent of n equals $k \geq 1$. Then the p -exponent of*

$$(p-1)^n + 1$$

equals $k+1$.

Proof. Because n is odd we get the binomial expansion

$$(p-1)^n + 1 = \binom{n}{n} - \binom{n}{n-1}p + \dots - \binom{n}{2}p^2 + \binom{n}{1}p.$$

The last term equals pn and therefore has p -exponent $k+1$. According to lemma 2 all other terms are divisible by p^{k+2} , we are done. □

We come back to the second step in the proof of IMO 90. We know that n is odd and divisible by 3. Assume that the 3-exponent of n equals k . One the one hand, by the above lemma with $p=3$, we know that the 3-exponent of $2^n + 1 = (3-1)^n + 1$ is $k+1$. On the other hand, this must be divisible by n^2 , whose 3-exponent is $2k$. We get $2k \leq k+1$, so $k=1$.

This lemma has many more applications. As an example we will compute the order of $p-1$ modulo powers of p .

Theorem 0.4. *Let $p \geq 3$ be a prime and $m \geq 1$ an integer. Then the order of $p-1$ modulo p^m equals $2 \cdot p^{m-1}$. Especially, 2 is a primitive root modulo all powers of 3.*

Proof. We are looking for the smallest positive integer d with

$$p^m \mid (p-1)^d - 1.$$

First, if n is odd, then $(p-1)^n - 1 \equiv -2 \not\equiv 0 \pmod{p}$, so d must be even. Now we use a trick. Because the order $d = 2e$ is even, we have that $(p-1)^e \equiv -1 \pmod{p^m}$. Therefore we are looking for the smallest positive integer e with

$$p^m \mid (p-1)^e + 1.$$

In other words, the smallest positive integer e , such that the p -exponent of $(p-1)^e + 1$ equals m . If n is even, then $(p-1)^n + 1 \equiv 2 \not\equiv 0 \pmod{p}$, so e is odd. We will use lemma 3. If the p -exponent of n is k , then the p -exponent of $(p-1)^n + 1$ is $k+1$. From this it is obvious that $e = p^{m-1}$ and we get $d = 2 \cdot p^{m-1}$, as claimed. □

Now we change the topic and make some considerations and applications of the notion of order mod m . In passing we will generalize and simplify some of the preceding considerations.

First we will compute the p -exponents of certain useful expressions. What follows is due to the proof of Theorem 5 and could therefore be skipped. But I recommend to study the proof because many important ideas come in. First we introduce a common notation. Let p be a prime and let m be an integer. We denote the p -exponent of m by $\text{ord}_p(m)$. This notation is used everywhere in algebra and number theory, but it is a bit confusing for you, maybe. Always remember that $\text{ord}_p(m)$ does NOT denote the order of $m \bmod p$ but it's p -exponent. For any fractional number $x = m/n$ we may define $\text{ord}_p(x) = \text{ord}_p(m) - \text{ord}_p(n)$. One easily checks that this does not depend on the choice of m and n and is therefore well defined. We will not use this for rational numbers, only for integers. The following formulas are valid for all integers m and n and all primes p :

- $\text{ord}_p(m) \geq 0$, and $\text{ord}_p(m) > 0$ if and only if m is divisible by p ,
- $\text{ord}_p(m \cdot n) = \text{ord}_p(m) + \text{ord}_p(n)$,
- $\text{ord}_p(m + n) \geq \min\{\text{ord}_p(m), \text{ord}_p(n)\}$, there is equality if $\text{ord}_p(m) \neq \text{ord}_p(n)$.

We are going to study p -exponents of expressions of the form $a^m - b^m$ in dependence of the p -exponents of $a - b$ and m .

First let p be an odd prime. Let a and b be two integers not divisible by p . For the following we will assume that $\text{ord}_p(a - b) \geq 1$, that means $a \equiv b \pmod{p}$. We are interested in the p -exponents of $a^m - b^m$ for natural numbers m . We distinguish two key cases:

First we assume that m is not divisible by p . Set $c = a - b$ and let $e = \text{ord}_p(c) \geq 1$. Consider the expansion

$$\begin{aligned} a^m - b^m &= (b + c)^m - b^m = \sum_{k=1}^m \binom{m}{k} c^k b^{m-k} \\ &= c^m + \binom{m}{m-1} c^{m-1} b + \dots + \binom{m}{2} c^2 b^{m-2} + m \cdot c b^{m-1}. \end{aligned}$$

Here the last term has p -exponent e (because m and b are not divisible by p by assumption), while all other terms are divisible by c^2 and therefore have p -exponents $\geq 2c > c$. We get

$$\text{ord}_p(a^m - b^m) = \text{ord}_p(a - b).$$

Next we consider the case $m = p$. Notations are as before. Now we get the expansion

$$\begin{aligned} a^p - b^p &= (b + c)^p - b^p = \sum_{k=1}^p \binom{p}{k} c^k b^{p-k} \\ &= c^p + \binom{p}{p-1} c^{p-1} b + \dots + \binom{p}{2} c^2 b^{p-2} + \binom{p}{1} c b^{p-1}. \end{aligned}$$

Here the first term is divisible by p^{pe} . Each of the following $p - 2$ terms is divisible by $p^{1+ke} \geq p^{1+2e}$, because all binomial coefficients are divisible by p . The last term however has p -exponent $e + 1$ (by assumption, b is not divisible by p). Taken together, this means that the p -exponent of $a^p - b^p$ is exactly $e + 1$, due to the inequalities $pe > e + 1$ and $1 + 2e > 1 + e$ (remember $p \geq 3$ and $e \geq 1$). So

$$\text{ord}_p(a^p - b^p) = \text{ord}_p(a - b) + 1.$$

combining and repeated application of these two cases gives the general formula

$$\text{ord}_p(a^n - b^n) = \text{ord}_p(a - b) + \text{ord}_p(n).$$

Next we look at $p = 2$. Assume that a and b are odd (then of course $\text{ord}_2(a - b) > 0$ automatically). Distinguish the same cases as above. The first one is verbatim the same as for $p \geq 3$. But in the second case we have now with $c = a - b$:

$$a^2 - b^2 = c^2 + 2bc.$$

If c is divisible by 4 then we get as before $\text{ord}_2(a^2 - b^2) = \text{ord}_2(a - b)$. If not, then write $c = 2d$ with d odd. We get $a^2 - b^2 = 4d^2 + 4bd = 4d(d + b)$ where the last bracket is even. So we have $\text{ord}_2(a^2 - b^2) \geq 3$.

Finally we will see what happens if $\text{ord}_p(a - b) = 0$. In this case the whole argumentation breaks down and in fact some additional phenomena appear. We don't describe them here in detail but content ourself with less. As a and b are not divisible by p , they have inverses mod p . Now

$$\text{ord}_p(a^n - b^n) > 0 \iff a^n \equiv b^n \pmod{p} \iff (ab^{-1})^n \equiv 1 \pmod{p}.$$

By assumption, $a \not\equiv b \pmod{p}$, so $ab^{-1} \not\equiv 1 \pmod{p}$. The order of $ab^{-1} \pmod{p}$ is therefore a divisor of $p - 1$ greater than 1. If n is coprime to $p - 1$, then n is surely not a multiple of this order. We get that

$$(n, p - 1) = 1 \implies \text{ord}_p(a^n - b^n) = 0.$$

Collecting everything we proved the following Theorem:

Theorem 0.5. *Let p be a prime number and let a and b be integers relatively prime to p . Let m be a positive integer.*

(a) *Assume that $a \equiv b \pmod{p}$.*

If $p \geq 3$ or $p = 2$ and $a \equiv b \pmod{4}$ or $p = 2$ and m is odd we have

$$\text{ord}_p(a^m - b^m) = \text{ord}_p(a - b) + \text{ord}_p(m).$$

If $p = 2$, m is even and $\text{ord}_2(a - b) = 1$ we have

$$\text{ord}_2(a^m - b^m) \geq \text{ord}_2(m) + 2.$$

(b) *Assume that $a \not\equiv b \pmod{p}$. If m is not a multiple of the order of $ab^{-1} \pmod{p}$, for example if m is relatively prime to $p - 1$, then*

$$a^m \not\equiv b^m \pmod{p}.$$

We get immediately interesting applications. A question related to some IMO problems is the following: If one has expressions of the form $a^m \pm b^m$ and $a^n \pm b^n$, what is the greatest common divisor? By factoring out if necessary we may assume that a and b are coprime. The case with the $-$ sign is already discussed in the script (bsp 27), but only in the special case $b = 1$. The proof there uses Bezout, but it does not seem to carry over to the general situation. We give an alternative approach.

Beispiel 1. Assume a and b are relatively prime integers, $a > b$, then

$$\gcd(a^m - b^m, a^n - b^n) = a^{\gcd(m,n)} - b^{\gcd(m,n)}.$$

Solution. First we may assume that m and n are relatively prime. If not let $d = (m, n)$ and replace a and b by a^d and b^d , as well as m and n by m/d and n/d . We need to prove that

$$(a^m - b^m, a^n - b^n) = a - b.$$

We do so by proving that both sides are divisible by the same prime powers. First we prove that both sides are divisible by the same primes. If p is a divisor of $a - b$ then it also divides the left hand side (by the binomial formulas or Theorem 5(a)). If p does not divide $a - b$, then it can not divide the left hand side. Assume it would, then by Theorem 5(b) both m and n would be divisible by the order $d > 1$ of $ab^{-1} \pmod p$, a contradiction since $(m, n) = 1$. Now let p be a prime divisor of both sides and let $e = \text{ord}_p(a - b)$ (then p must be odd!). By Theorem 5(a) the p -exponent of the left hand side equals $e + \min\{\text{ord}_p(m), \text{ord}_p(n)\}$. But either m or n is not divisible by p , so $\text{ord}_p(m) = 0$ or $\text{ord}_p(n) = 0$, giving the desired result. \square

From this many related gcd's can be computed (compare the discussion in the script on cyclotomic polynomials). For this we need a trivial but useful observation: Let a, b and c be integers, then

$$(ab, c) \mid (a, c)(b, c), \quad \text{there is equality if } a \text{ and } b \text{ are coprime.}$$

Indeed, write $d = (a, c), e = (b, c)$ and $a = xd, b = ye$. Then $(ab, c) = (dexy, c) = (de, c) \mid de = (a, c)(b, c)$ with equality if $de \mid c$, which is true if a and b are coprime.

Again, let a and b be coprime. In the factorization

$$a^{2m} - b^{2m} = (a^m - b^m)(a^m + b^m)$$

the two terms on the right hand side are coprime. Using the above result together with example 1 we get

$$\begin{aligned} a^{(2m,n)} - b^{(2m,n)} &= (a^{2m} - b^{2m}, a^n - b^n) \\ &= (a^m - b^m, a^n - b^n)(a^m + b^m, a^n - b^n) \\ &= (a^{(m,n)} - b^{(m,n)})(a^m + b^m, a^n - b^n), \end{aligned}$$

and therefore

$$(a^m + b^m, a^n - b^n) = \frac{a^{(2m,n)} - b^{(2m,n)}}{a^{(m,n)} - b^{(m,n)}}.$$

Continuing this way a computation gives

$$\begin{aligned} a^{2(m,n)} - b^{2(m,n)} &= (a^{2m} - b^{2m}, a^{2n} - b^{2n}) \\ &= ((a^m - b^m)(a^m + b^m), (a^n - b^n)(a^n + b^n)) \\ &= \dots \\ &= (a^{(m,n)} - b^{(m,n)}) \cdot \frac{a^{(2m,n)} - b^{(2m,n)}}{a^{(m,n)} - b^{(m,n)}} \cdot \frac{a^{(m,2n)} - b^{(m,2n)}}{a^{(m,n)} - b^{(m,n)}} \cdot (a^m + b^m, a^n + b^n), \end{aligned}$$

and therefore

$$(a^m + b^m, a^n + b^n) = \frac{(a^{2(m,n)} - b^{2(m,n)}) \cdot (a^{(m,n)} - b^{(m,n)})}{(a^{(2m,n)} - b^{(2m,n)}) \cdot (a^{(m,2n)} - b^{(m,2n)})}.$$

To evaluate this monster we have to distinguish several cases according to the 2-exponents of m and n . For example we have $a^{(2m,n)} - b^{(2m,n)} = a^{(m,n)} - b^{(m,n)}$ or $= a^{2(m,n)} - b^{2(m,n)}$ depending on whether $\text{ord}_2(m) \geq \text{ord}_2(n)$ or $\text{ord}_2(m) < \text{ord}_2(n)$. As a result we obtain

Beispiel 2. Let a and b be coprime, then

$$(a^m + b^m, a^n + b^n) = \begin{cases} a^{(m,n)} + b^{(m,n)}, & \text{if } \text{ord}_2(m) = \text{ord}_2(n); \\ 1, & \text{if } \text{ord}_2(m) \neq \text{ord}_2(n). \end{cases}$$

The most important special case is when $b = 1$ and m and n are odd and coprime. Then we get

$$(a^m + 1, a^n + 1) = a + 1, \quad \text{for example} \quad (2^m + 1, 2^n + 1) = 3.$$

As a next application of Theorem 5, we get again Lemma 3, which is now only a trivial consequence. In fact, set $a = p-1$, $b = -1$ and $m = n$ in Theorem 5(a), then the assumptions are fulfilled and we have that (m is odd!)

$$\text{ord}_p((p-1)^n + 1) = \text{ord}_p((p-1)^n - (-1)^m) = \text{ord}_p(p) + \text{ord}_p(n) = \text{ord}_p(n) + 1.$$

We may also give a new proof of Theorem 4. We need to find the smallest integer $d > 1$ such that $\text{ord}_p((p-1)^d - 1) \geq m$. Obviously d must be even and we set $d = 2e$. Now $(p-1)^d - 1 = (p^2 - 2p + 1)^e - 1$. We use Theorem 5(a) with $a = p^2 - 2p + 1$ and $b = 1$ and get

$$\text{ord}_p((p^2 - 2p + 1)^e - 1) = \text{ord}_p((p^2 - 2p + 1) - 1) + \text{ord}_p(e) = \text{ord}_p(e) + 1.$$

This gives immediately $e = p^{m-1}$ and $d = 2 \cdot p^{m-1}$, as desired.

Another consequence of the fact that 2 is a primitive root modulo all powers of 3:

Beispiel 3. There are infinitely many positive integers n such that n is a divisor of $2^n + 1$. Indeed, this is true for $n = 3^k$.

Solution. The order of 2 mod 3^k equals $2 \cdot 3^{k-1}$, so the order of $2^{3^{k-1}}$ mod 3^k equals 2. This gives (mod 3^k)

$$2^{3^{k-1}} \equiv -1 \implies 2^{3^k} \equiv (-1)^3 = -1 \iff 3^k \mid 2^{3^k} + 1.$$

□

Exercises

1. (SMO 03) Find the largest positive integer n , that divides $a^{25} - a$ for all integers a .
2. (IMO 01) Find all pairs (n, p) of positive integers, such that
 - (a) p is a prime number,
 - (b) $n \leq 2p$,
 - (c) $(p - 1)^n + 1$ is divisible by n^{p-1} .
3. (IMO 2000) Decide whether there exists a positive integer n having exactly 2000 different prime divisors, such that $n \mid 2^n + 1$.
4. (USA TST 03) Find all triples (p, q, r) of prime numbers, such that

$$p \mid q^r + 1, \quad q \mid r^p + 1, \quad r \mid p^q + 1.$$

5. (IMO 03) Let p be a prime number. Prove that there exists a prime number q , such that

$$q \nmid n^p - p, \quad \text{for all integers } n.$$