

This was probably the highest-scoring homework this semester. People had problems with #1 (Just read the solution), #4b and #5, and there was some confusion about applying quadratic reciprocity. I hope it's clear now.

Math 453
HW6
Extra Problems

Mr. Zhang had a clever proof that's a variation on #5 that does not use the hint.

If $u \equiv 1 \pmod{m}$ and $u \equiv 0 \pmod{n}$, then $(m-1)u \equiv m-1 \equiv -1 \pmod{m}$ and $(m-1)u \equiv (m-1) \cdot 0 \equiv 0 \pmod{n}$
 so let $v = (m-1)u + 1$, then $v \equiv -1 + 1 \equiv 0 \pmod{m}$ and $v \equiv 0 + 1 \equiv 1 \pmod{n}$

What's going on?

Well, $n \mid u$ so $m-n \mid mu$ and $(m-1)u + 1 = mu - u + 1 \equiv 0 - u + 1 \equiv (-u) \pmod{n}$

A different solution that failed the grader!

On 4b. What can we "expect" $v_2(n!)$ to be?

It's exactly $\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \dots$, which is a little smaller than $\frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \dots = \frac{n}{p} (1 + \frac{1}{p} + \frac{1}{p^2} + \dots) = \frac{n}{p} \frac{1}{1 - \frac{1}{p}} = \frac{n}{p-1}$

so we can expect $v_2(n!)$ to be about n and $v_3(n!)$ to be about $\frac{n}{2}$. So we can "expect" that $12^{n/2}$ (or a little less)

divides $n!$. Sometimes $v_2(n!) > 2 \cdot v_3(n!)$ as with $n=100$ ($97 > 2 \cdot 48$), sometimes it's the other way around: For example, if $n=9$, $v_2(9!) = 7$ and $v_3(9!) = 4$ and $7 < 2 \cdot 4$.

#1 Alternate solution

$$ax^2 + bx + c \equiv 0 \pmod{m}$$

multiply by $4a$

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am}$$

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{4am}$$

so $3x^2 + 2x + 13 \equiv 0 \pmod{17}$

$$4a = 12$$

$$36x^2 + 24x + 156 \equiv 0 \pmod{17}$$

$$(6x + 2)^2 \equiv 4 - 156 = -152 \equiv 1 \pmod{17}$$

$$\Rightarrow (6x + 2)^2 \equiv 1 \pmod{17}, 6x + 2 \equiv 1, -1$$

$$6x \equiv -1, -3 \pmod{17}, 6^{-1} \equiv 3 \pmod{17}$$

so $3 \cdot 6x \equiv -3, -9 \pmod{17}$, or $x \equiv 14, 8 \pmod{17}$

$$2x^2 + x \equiv 5 \pmod{23}$$

Other way: $2^{-1} \equiv 12 \pmod{23}$

$$24x^2 + 12x \equiv 60 \pmod{23}$$

$$x^2 + 12x + 36 \equiv 60 + 36 \pmod{23}$$

$$(x + 6)^2 \equiv 96 \equiv 4 \equiv 2^2 \pmod{23}$$

$$\Rightarrow x + 6 \equiv 2 \pmod{23}$$

$$x + 6 \equiv -2 \pmod{23}$$

$$x \equiv -4, -8 \pmod{23}, \text{ or } x \equiv 15, 19.$$

#2 Always check whether an odd n is prime.

87 and 91 aren't prime!

#3 Look at the solution.

Remember $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

if p and q are prime, and

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \text{ if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4}$$

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \text{ if } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4}$$

#4. Be sure you're doing the correct problem.

Math 453
HW 7
Bonus

#5 done the other way.

$$3n^2 + 5n + 8 \equiv 0 \pmod{29}$$

multiply by $4a = 12$

$$36n^2 + 60n + 96 \equiv 0 \pmod{29}$$

$$(6n + 5)^2 \equiv 25 - 96 \pmod{29}$$
$$\equiv -71 \equiv 16 \pmod{29}$$

so $6n + 5 \equiv 4 \pmod{29}$

$$6n + 5 \equiv -4 \pmod{29}$$

$$6n \equiv -1 \pmod{29}$$

$$6n \equiv -9 \pmod{29}$$

$$6^{-1} \equiv 5 \pmod{29}, \text{ so}$$

$$30n \equiv n \equiv -5 \pmod{29}$$

$$30n \equiv n \equiv -45 \pmod{29}$$

$$-5 \equiv 24 \pmod{29} \quad -45 \equiv 13 \pmod{29}$$

Note: $x^2 \equiv a \pmod{p}$ has 0 or 2 solutions.

If you recognize $a = m^2 \pmod{p}$ then $x \equiv m$ and $x \equiv -m$ are solutions, and they have to be the only ones.

#6, 7 If you see $x^2 \equiv 1 \pmod{p}$, you can just write down $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$

I hope this is all clearer after our class discussions.

#1. If there are primitive roots mod n , there are $\phi(\phi(n))$ of them. If there aren't, there are none!

#2. As always, these equations mod p , turn into an equation mod $\phi(p)$.

#3. Only 3 or 4 more serious progress on this one.

It's not that hard if you think about it from the right point of view. You always have $\text{ord}_p a \mid p-1$ for a prime p and a with $\text{gcd}(a, p) = 1$. If $p-1$ has a special form, this can give useful information.

#4. Many ways to do this.

Recall: $\text{ord}_m a^k = \frac{\text{ord}_m a}{\text{gcd}(\text{ord}_m a, k)}$

a useful formula!

#5. The method of this example shows that if $\text{gcd}(m_i, m_j) = 1$ for $1 \leq i \neq j \leq n$, then

$$\text{ord}_{m_1 \cdots m_n} a = \text{lcm}(\text{ord}_{m_1} a, \dots, \text{ord}_{m_n} a)$$

#6. I didn't write down the actual values, so here they are.

$$\begin{aligned} 3^{44} &\equiv 1 \pmod{353} \\ 3^{11} &\equiv -70 \pmod{353} \\ 3^{22} &\equiv -42 \pmod{353} \\ 3^{33} &\equiv 116 \pmod{353} \\ 3^{44} &\equiv -1 \pmod{353} \\ 3^{55} &\equiv 70 \pmod{353} \\ 3^{66} &\equiv 42 \pmod{353} \\ 3^{77} &\equiv -116 \pmod{353} \end{aligned}$$

Math 453
HW 8 Extra

#7 Alternate. According to table 5.1
6 is the least primitive root mod 41.

So $x^4 \equiv 1 \pmod{41}$ $x = 6^r$
 $6^{4r} \equiv 1 \pmod{41}$

$$\Leftrightarrow 4r \equiv 0 \pmod{40}$$

$$\Leftrightarrow r \equiv 0 \pmod{10}$$

$$x \equiv 6^0, 6^{10}, 6^{20}, 6^{30} \pmod{41}$$

1	32	40	9

I couldn't reasonably expect anything but $6^0, 6^{10}, 6^{20}, 6^{30}$ on an exam.

$$x^4 \equiv 16 \pmod{41}, x = 6^r$$

$$16 \equiv 6^{24} \pmod{41}. \text{ (This would have to be given to you.)}$$

$$6^{4r} \equiv 6^{24} \pmod{41}$$

$$\Leftrightarrow 4r \equiv 24 \pmod{40}$$

$$\Leftrightarrow r \equiv 6 \pmod{10}$$

$$x = 6^6, 6^{16}, 6^{26}, 6^{36} \pmod{41}$$

39	18	2	23

Mathematica did the calculations.

1. A hard assignment. I used 1.2.11
 turned it in.

2. It's important to review the distinction between primitive roots and quadratic non-residues.

Suppose $p \geq 3$ is a prime. We know that there exists a primitive root - call it r . $\text{ord}_p r = \phi(p) = p-1$

So: $1, r, r^2, \dots, r^{p-1}$ run through all congruence classes mod p (except 0). If $\text{gcd}(a, p) = 1$, then $\exists k, 0 \leq k \leq p-1$

So that $a \equiv r^k \pmod p$ (I won't use the index notation.)

(i) Quadratic Reciprocity.

$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ by Fermat's theorem, so $a = r^k$, and

$$\left(\frac{a}{p}\right) = r^{k \cdot \frac{p-1}{2}} \pmod p.$$

$$\text{Thus } \left(\frac{a}{p}\right) = 1 \iff \phi(p) \mid k \cdot \frac{p-1}{2} \iff p-1 \mid k \cdot \frac{p-1}{2} \iff \frac{k}{2} \in \mathbb{Z} \iff 2 \mid k$$

The quadratic residues are $r^2, r^4, r^6, \dots, r^{p-1}$ (r^{2k})

The quadratic non-residues are $r^1, r^3, r^5, \dots, r^{p-2}$ (r^{2k+1}).

(ii) $\text{ord}_p a^k = \frac{\text{ord}_p a}{\text{gcd}(\text{ord}_p a, k)} = \frac{p-1}{\text{gcd}(p-1, k)}$, so a^k is a primitive

root $\iff \text{gcd}(k, p-1) = 1$. Since p is an odd prime, $2 \mid p-1$ and

This implies that k is odd, but is more restrictive.

3 Example Let $p = 19$. Suppose a is a primitive root.

(i) Quadratic Residues: $r^2, r^4, r^6, r^8, r^{10}, r^{12}, r^{14}, r^{16}, r^{18}$ $\phi(\phi(19)) = \phi(18) = 6$

(ii) Quadratic Non-residues: $r, r^3, r^5, r^7, r^9, r^{11}, r^{13}, r^{15}, r^{17}$

(iii) Primitive Roots: $r, r^5, r^7, r^{11}, r^{13}, r^{17}$ 3, 9, and 15 are odd but aren't rel. prime to 19-1.

The book says 2 is a primitive root mod 19, hence others are $2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$ or 13, 4, 15, 3, 10.

You can say that if Γ is a primitive root, then $\text{ord}_p(\Gamma) = p-1$.

Other comments on the

#1. $\text{ord}_p(\Gamma) = p-1$ when $p-1$ has a nice shape, this limits the method.

#2 you should be able to do those problems

#3 Read the question carefully.

If $8x + 13y = 1571$, then arithmetically,

$$x, y \geq 0$$

$$8x + 8y \leq 8x + 13y \leq 13x + 13y$$

$$8(x+y) \leq 1571 \leq 13(x+y)$$

so $\frac{1571}{13} \leq x+y \leq \frac{1571}{8}$. This gives a range of answers.

I don't trust a \$8 steak or a \$13 lobster.

#4 I really didn't think this was a hard problem. I was apparently wrong.

#5 Most people got this

#6 Done in class. See comments at beginning.

#7. Pretty straightforward.

#8 Only one person tried it, and it's easy!

An alternative proof. If $p \mid x$, then $p \mid x^2 + py^2$ so $p \mid az^2$

If $p \mid z$, then $p \mid x^2 + py^2 \Rightarrow p \mid x^2 \Rightarrow p \mid x$ so $p \mid z^2$ so $p \mid z$

$$\text{If } p \nmid x, \text{ then } 1 = \left(\frac{x^2}{p}\right) = \left(\frac{x^2 + py^2}{p}\right) = \left(\frac{az^2}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{z^2}{p}\right) = \left(\frac{z^2}{p}\right) = -1$$

which is a contradiction

The "point-slope" method generalizes to many other

Diophantine equations like $x^2 + y^2 = z^2$, as long as

they are "homogeneous" of degree 2.

Math 453 Bonus Notes Oct. 22, 2007

For an integer $m \geq 1$, let $N(m)$ denote the number of incongruent solutions to $x^2 \equiv 1 \pmod{m}$. In these notes, we'll completely analyze $N(m)$.

(i) Suppose $\gcd(m, n) = 1$. Then

$$x^2 \equiv 1 \pmod{mn} \iff \begin{cases} x^2 \equiv 1 \pmod{m} \\ x^2 \equiv 1 \pmod{n} \end{cases}$$

So, as in the Chinese Remainder Theorem, each solution to $x^2 \equiv 1 \pmod{m}$ and to $x^2 \equiv 1 \pmod{n}$ corresponds to a solution \pmod{mn} . Thus $N(mn) = N(m)N(n)$.

Ex
 $m=3, n=5$ $x^2 \equiv 1 \pmod{3} \iff x \equiv 1 \pmod{3} \text{ or } x \equiv 2 \pmod{3}$
 $x^2 \equiv 1 \pmod{5} \iff x \equiv 1 \pmod{5} \text{ or } x \equiv 3 \pmod{5}$

$N(15) = N(3) \cdot N(5)$

	CRT	$1 \pmod{5}$	$4 \pmod{5}$	$1^2 = 1$
(!)	$1 \pmod{3}$	$1 \pmod{15}$	$4 \pmod{15}$	$4^2 = 16 \equiv 1 \pmod{15}$
	$2 \pmod{3}$	$11 \pmod{15}$	$14 \pmod{15}$	$11^2 = 121 \equiv 1 \pmod{15}$
				$14^2 = 196 \equiv 1 \pmod{15}$

(ii) Suppose $p \geq 3$ is prime and $x^2 \equiv 1 \pmod{p^a}$, $a \geq 1$. Then $p^a \mid x^2 - 1 = (x-1)(x+1)$. If $p \mid x-1$ and $p \mid x+1$ then $p \mid (x+1) - (x-1) = 2$, which is impossible. Thus, either $p^a \mid x-1$ ($x \equiv 1 \pmod{p^a}$) or $p^a \mid x+1$ and $x \equiv -1 \equiv p^a - 1 \pmod{p^a}$, and $N(p^a) = 2$. (See above for $p=3, 5$.)

(iii) For $p=2$, the situation is a bit trickier. $x^2 \equiv 1 \pmod{2^a}$, $a \geq 1$ means that x is odd

$a=1$	$x^2 \equiv 1 \pmod{2}$	$a=2$	$x^2 \equiv 1 \pmod{4}$	$a=3$	$x^2 \equiv 1 \pmod{8}$
	\iff		$1^2 = 1 \equiv 1 \pmod{4}$		$1^2 = 1 \equiv 1 \pmod{8}$
	$x \equiv 1 \pmod{2}$		$3^2 = 9 \equiv 1 \pmod{4}$		$5^2 = 25 \equiv 1 \pmod{8}$
					$7^2 = 49 \equiv 1 \pmod{8}$

(over)

Thus, by direct calculation, $N(2) = 1$, $N(4) = 2$, $N(8) = 4$

Consider $x^2 \equiv 1 \pmod{2^a}$, $a \geq 3$.

$2^a \mid (x^2 - 1) = (x-1)(x+1)$, so $a \leq v_2(x-1) + v_2(x+1)$.

As in (ii), $2^k \mid x-1$ and $2^k \mid x+1 \Rightarrow 2^k \mid (x+1) - (x-1) = 2$

so $k \leq 1$; That is, $\min(v_2(x-1), v_2(x+1)) = 0$ or 1

Since $v_2(x-1) + v_2(x+1) \geq a$ and $\min(v_2(x-1), v_2(x+1)) = 0$ or 1

it follows that $\max(v_2(x-1), v_2(x+1)) \geq a-1$, so either $2^{a-1} \mid x-1$ or $2^{a-1} \mid x+1$.

If $2^{a-1} \mid x-1$, then $x \equiv 1 \pmod{2^{a-1}}$ and since $2^a = 2 \cdot 2^{a-1}$, this means that $x \equiv 1$ or $1 + 2^{a-1} \pmod{2^a}$.

If $2^{a-1} \mid x+1$, then $x \equiv -1 \equiv 2^{a-1} - 1 \pmod{2^a}$ and so $x \equiv 2^{a-1} - 1$ or $2^{a-1} + 1 \pmod{2^a}$.

To sum up: If $a \geq 3$, $N(2^a) = 4$ and $x^2 \equiv 1 \pmod{2^a} \Leftrightarrow x \equiv \pm 1, \pm(2^{a-1} - 1) \pmod{2^a}$.

Eg $a = 5$ $1^2 \equiv 1 \pmod{32}$, $15^2 = 225 \equiv 1 \pmod{32}$.

$2^{a-1} = 16$ $9^2 = 81 \equiv 1 \pmod{32}$, $17^2 = 289 \equiv 1 \pmod{32}$

(iv). If $n = p_1^{a_1} \dots p_r^{a_r}$, then $N(n) = N(p_1^{a_1}) \dots N(p_r^{a_r})$

where $N(2^1) = 1$, $N(2^a) = 4$, $a \geq 3$

$N(2^2) = 2$, $N(p^a) = 2$, $p \geq 3$, $a \geq 1$.

(iv) Ex $n = 24 = 2^3 \cdot 3$ $N(24) = N(2^3) \cdot N(3) = 4 \cdot 2 = 8$.

	1 mod 8	3 mod 8	5 mod 8	7 mod 8	
1 mod 3	1 mod 24	19 mod 24	13 mod 24	7 mod 24	← 8 solutions
2 mod 3	17 mod 24	11 mod 24	5 mod 24	23 mod 24	

As a check: $1^2 = 1$, $5^2 = 25 = 1 \cdot 24 + 1$, $7^2 = 49 = 2 \cdot 24 + 1$,

$11^2 = 121 = 5 \cdot 24 + 1$, $13^2 = 169 = 7 \cdot 24 + 1$, $17^2 = 289 = 12 \cdot 24 + 1$

$19^2 = 361 = 15 \cdot 24 + 1$, $23^2 = 529 = 22 \cdot 24 + 1$.

Math 453 - Writing integers based + a bonus! 11/12/07

1. We ordinarily write integers in base 10, so that $453 = 4 \times 10^2 + 5 \times 10^1 + 3 \times 10^0$. For these numbers, if no base is written, then it's base 10. But it doesn't have to be! Fix $d \geq 2$ an integer.

Theorem positive

Every integer n can be written in a unique way

as
$$n = \sum_{i=0}^m a_i \cdot d^i \text{ with } a_i \in \{0, \dots, d-1\}$$

and $a_m > 0$.

We call this the base d representation and write

$$n = [a_m a_{m-1} \dots a_1 a_0]_d$$

For example, $453 = 7 \times 8^2 + 0 \times 8^1 + 5 \times 8^0$, so

$$453 = [705]_8$$

Proof.

Induction on n . If $1 \leq n \leq d-1$, then set $m=0$ and $a_0 = n$ and $n = [n]_d$ automatically.

Suppose the theorem is valid for all $n \leq n_0 - 1$, $n_0 \geq d$.

By the division algorithm, we can write

$$n_0 = n \cdot d + a_0, \quad a_0 \in \{0, \dots, d-1\}$$

Since $n_0 \geq d$, $n \geq 1$ and $n < n_0$, so by the induction hypothesis,

$$n = \sum_{i=0}^m b_i d^i = b_0 + b_1 d + \dots + b_m d^m$$

$$\text{and } n_0 = a_0 + d n = a_0 + b_0 d + b_1 d^2 + \dots + b_m d^{m+1}$$

Thus, there is at least one such representation.

Suppose there were two.

$$\boxed{a_0 + a_1 d + \dots + a_m d^m = b_0 + b_1 d + \dots + b_n d^n}$$

$a_i, b_i \in \{0, 1, \dots, d-1\}$. Take this equation mod d .

$a_0 \equiv b_0 \pmod{d}$. Since $0 \leq a_0, b_0 \leq d-1$, we must have $a_0 = b_0$. Subtract these from the boxed equation and divide by d .

$$a_1 + a_2 d + \dots + a_m d^{m-1} = b_1 + b_2 d + \dots + b_n d^{n-1}$$

A similar argument shows that $a_i = b_i$, etc.

2. The recursive construction of $[n]_d$.

We have

$$\begin{aligned} 453 &= 8 \cdot 56 + 5 \\ 56 &= 8 \cdot 7 + 0 \\ 7 &= 8 \cdot 0 + 7 \end{aligned}$$

$$453 = [705]_8$$

so

$$453 = 5 + 8(56) = 5 + 8(0 + 8 \cdot 7) = 5 + 0 \cdot 8 + 7 \cdot 8^2$$

This works for any number and any base.

Eg.

$$\begin{aligned} 2007 &= 7 \cdot 286 + 5 \\ 286 &= 7 \cdot 40 + 6 \\ 40 &= 7 \cdot 5 + 5 \\ 5 &= 7 \cdot 0 + 5 \end{aligned}$$

$$\begin{aligned} 2007 &= 7 \cdot 286 + 5 = 7(7 \cdot 40 + 6) + 5 \\ &= 7(7(7 \cdot 5 + 5) + 6) + 5 = 7^3 \cdot 5 + 7^2 \cdot 6 + 7 \cdot 5 \\ &= [5565]_7. \end{aligned}$$

Note that you read UP the remainders.

3. The odometer effect

If $n = d^k \cdot n'$ and $n' = [a_r \dots a_0]_d$, then

$$n = d^k n' = [a_r \dots a_0 \underbrace{0 \dots 0}_k \text{ zeros}]_d$$

with $a_0 > 0$

and, this is key, $n-1 = [a_r \dots a_0]_d \frac{d-1}{k}$

You know this when $d=10$.

Eg $n=25000 = 10^3 \cdot 25$ has $n-1 = 24999$.

4. A strangely useful function

Let $f_d(n) = \sum_{i=0}^m a_i$ be the sum of the digits in the base d representation of n . We have, based on the examples here

$$f_{10}(2007) = 2+0+0+7=9, \quad f_7(2007) = 5+5+6+5=21$$

$$f_{10}(453) = 4+5+3=12, \quad f_8(453) = 7+0+5=12$$

We are really interested in $f_d(n) - f_d(n-1)$.

(a) If $d \nmid n$ and $[n-1]_d = [a_m \dots a_1 a_0]_d$
Then $[n]_d = [a_m \dots a_1 a_0 + 1]_d$

$$\text{So that } f_d(n) = f_d(n-1) + 1$$

If $d^k \mid n$ and $d^{k+1} \nmid n$, then

$$[n-1]_d = [a_m \dots a_k d-1 \dots d-1]_d$$

$$[n]_d = [a_m \dots a_{k+1} 0 \dots 0]_d$$

This is the odometer clock

$$f_d(n) = f_d(n-1) + 1 - k(d-1)$$

This is true for any d , whether prime or composite, and taking $k=0$, we have...

THM Suppose $k \geq 0$ and $d^k \mid n$ but $d^{k+1} \nmid n$. Then

$$f_d(n) = f_d(n-1) + 1 - k(d-1)$$

5. Payoff

Theorem (Better than De Polignac!)

If p is a prime, Then

$$L_p(n!) = \frac{n - f_p(n)}{p-1}$$

Proof.

Induction on n . $L_p(1!) = 0$

$$f_p(1) = 1 \text{ and } 0 = \frac{1-1}{p-1}.$$

Suppose valid for $n-1$, so

$$L_p((n-1)!) = \frac{n-1 - f_p(n-1)}{p-1}$$

By the last Theorem, $f_p(n) = f_p(n-1) + 1 - L_p(n)(p-1)$

$$\begin{aligned} \text{So } \frac{n - f_p(n)}{p-1} &= \frac{n - (f_p(n-1) + 1 - L_p(n)(p-1))}{p-1} \\ &= \frac{n-1 - f_p(n-1)}{p-1} + L_p(n) \cdot \frac{p-1}{p-1} \\ &= L_p((n-1)!) + L_p(n) \\ &= L_p(n \cdot (n-1)!) = L_p(n!). \end{aligned}$$

$$\text{Eg. } L_7(2007!) = \frac{2007 - 21}{7-1} = \frac{1986}{6} = 331$$

We can check this by The division algorithm:

$$L \left\lfloor \frac{2007}{7} \right\rfloor = L \left\lfloor 286 \frac{5}{7} \right\rfloor = 286, \quad L \left\lfloor \frac{2007}{49} \right\rfloor = L \left\lfloor 40 + \frac{6}{7} + \frac{5}{7^2} \right\rfloor = 40$$

$$L \left\lfloor \frac{2007}{343} \right\rfloor = L \left\lfloor 5 + \frac{5}{7} + \frac{6}{7^2} + \frac{5}{7^3} \right\rfloor = 5, \quad L \left\lfloor \frac{2007}{2401} \right\rfloor = 0, \text{ etc.}$$

$$286 + 40 + 5 = 331$$

By the way, 331 is prime and the smallest p s.t. $\binom{k}{p} = 1$ for $1 \leq k \leq 10!$