

<u>prime</u>	<u>equation</u>	<u>solutions</u>
$p=2$	$x^2 \equiv n \pmod{2}$	$x \equiv 1$
$p=3$	$x^2 \equiv n \pmod{3}$	none
$p=5$	$x^2 \equiv n \pmod{5}$	$x \equiv 1, 4$
$p=7$	$x^2 \equiv n \pmod{7}$	none
$p=11$	$x^2 \equiv n \pmod{11}$	$x \equiv 1, 10$
$p=13$	$x^2 \equiv n \pmod{13}$	$x \equiv 2, 11$

$$n = 2201$$

	<u>prime</u>	<u>equation</u>	<u>solutions</u>
Factor Base	$p = 2$	$x^2 \equiv n \pmod{2}$	$x \equiv 1$
	$p = 3$	$x^2 \equiv n \pmod{3}$	none
	$p = 5$	$x^2 \equiv n \pmod{5}$	$x \equiv 1, 4$
	$p = 7$	$x^2 \equiv n \pmod{7}$	none
	$p = 11$	$x^2 \equiv n \pmod{11}$	$x \equiv 1, 10$
	$p = 13$	$x^2 \equiv n \pmod{13}$	$x \equiv 2, 11$

$$n = 2201$$

$$n = 2201$$

$$\sqrt{n} \approx 47$$

$$n = 2201$$

$$\sqrt{n} \approx 47$$

k 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63

$$n = 2201$$

$$\sqrt{n} \approx 47$$

k	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768

k	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2-n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768

$k \bmod 2$  1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1

$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768

$k \bmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \bmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3

$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768



$k \bmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \bmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \bmod 11$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \bmod 13$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11
$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768

$k \bmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \bmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \bmod 11$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \bmod 13$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11
$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768

highlight  $k$  such that  
 $k^2 \equiv n \pmod{2}$   
 has solutions

$k \bmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \bmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \bmod 11$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \bmod 13$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11
$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768

highlight  $k$  such that  
 $k^2 \equiv n \pmod{2}$   
 has solutions



$$2 \mid k^2 - n$$

$k \bmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \bmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \bmod 11$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \bmod 13$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11
$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768

↓  
4

$k \bmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \bmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \bmod 11$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \bmod 13$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11
$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768

↓  
4  
↓  
2  
↓  
1





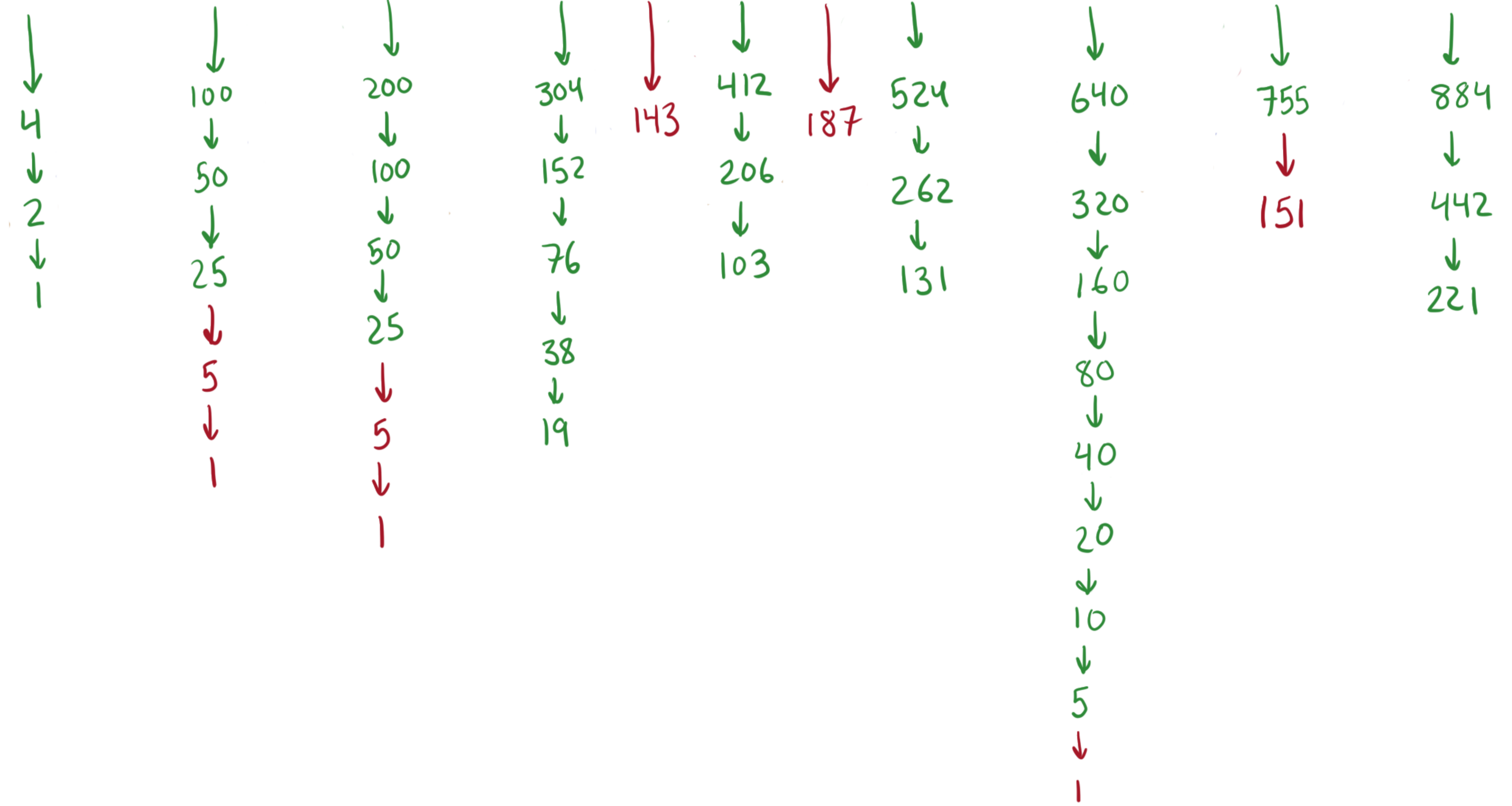
$k \bmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \bmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \bmod 11$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \bmod 13$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11
$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768
	↓		↓		↓		↓		↓		↓		↓		↓		↓
	4		100		200		304		412		524		640		755		884
	↓		↓		↓		↓		↓		↓		↓				↓
	2		50		100		152		206		262		320				442
	↓		↓		↓		↓		↓		↓		↓				↓
	1		25		50		76		103		131		160				221
					↓		↓						↓				
					25		38						80				
							↓						↓				
							19						↓				
													40				
													↓				
													20				
													↓				
													10				
													↓				
													5				



$k \bmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \bmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \bmod 11$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \bmod 13$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11
$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768
	↓		↓		↓		↓		↓		↓		↓		↓		↓
	4		100		200		304		412		524		640		755		884
	↓		↓		↓		↓		↓		↓		↓				↓
	2		50		100		152		206		262		320				442
	↓		↓		↓		↓		↓		↓		↓				↓
	1		25		50		76		103		131		160				221
					↓		↓						↓				
					25		38						80				
							↓						↓				
							19						↓				
													40				
													↓				
													20				
													↓				
													10				
													↓				
													5				

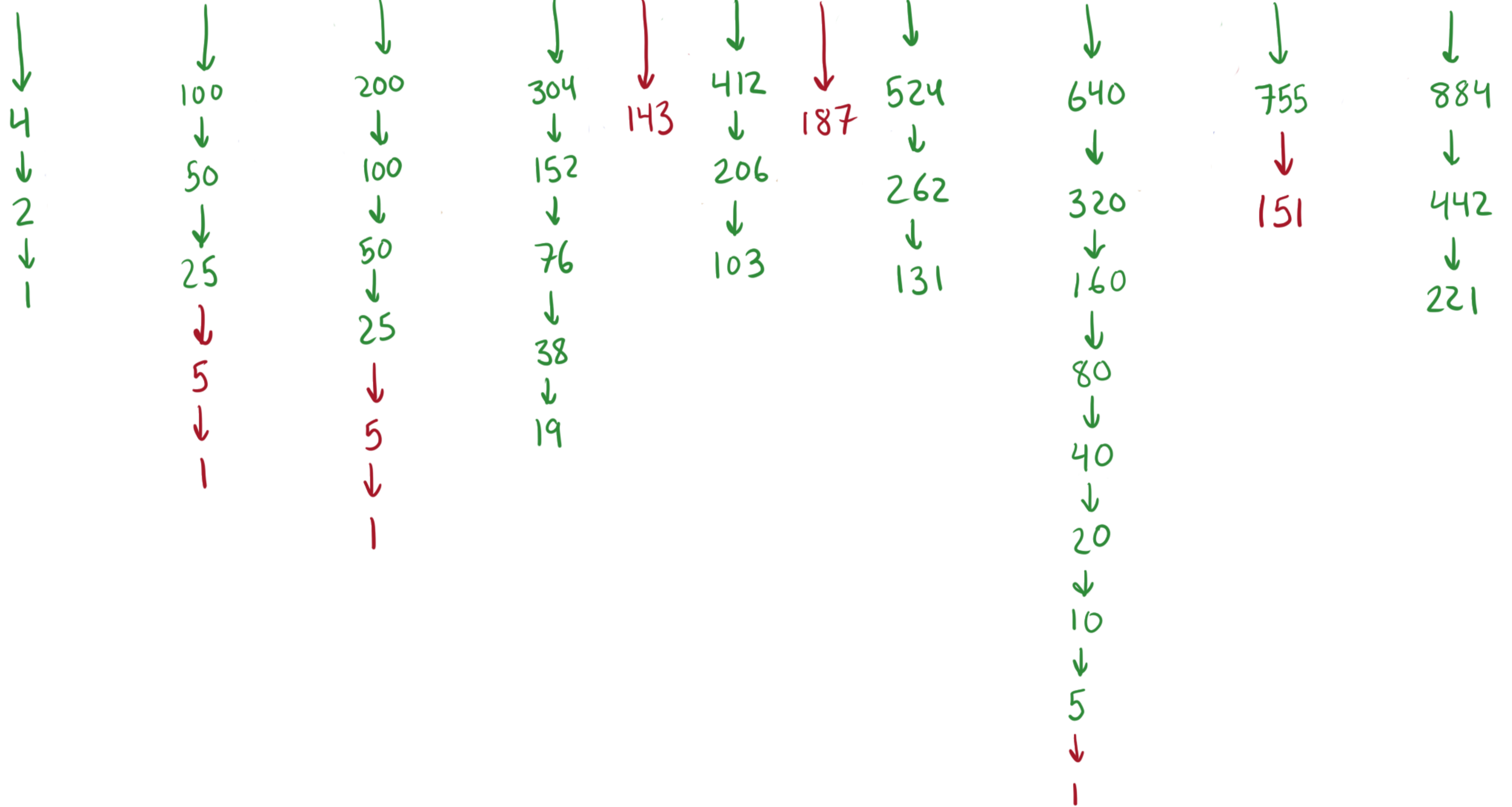
$k \pmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \pmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \pmod{11}$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \pmod{13}$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11

$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768



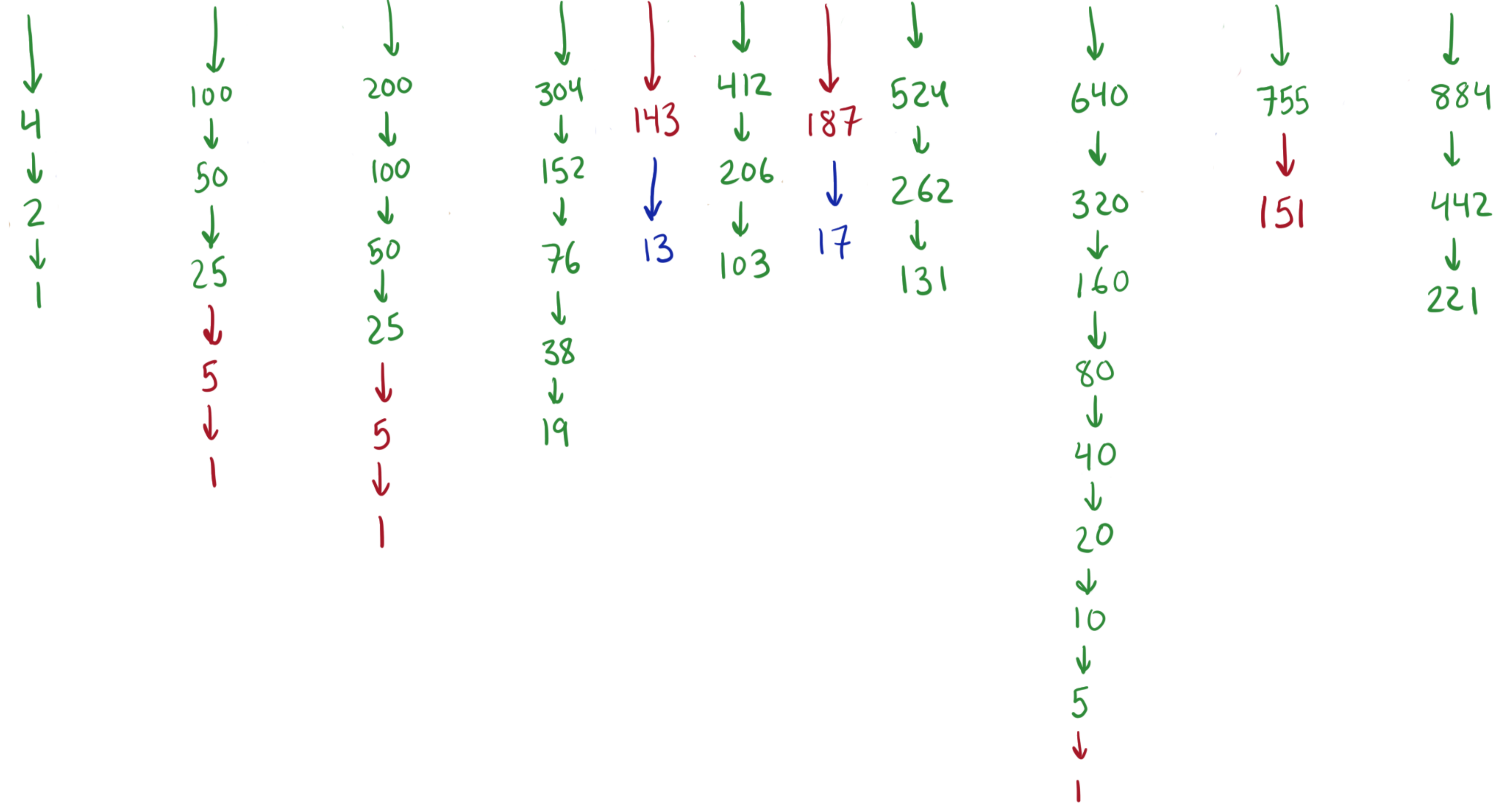
$k \pmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \pmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \pmod{11}$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \pmod{13}$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11

$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768



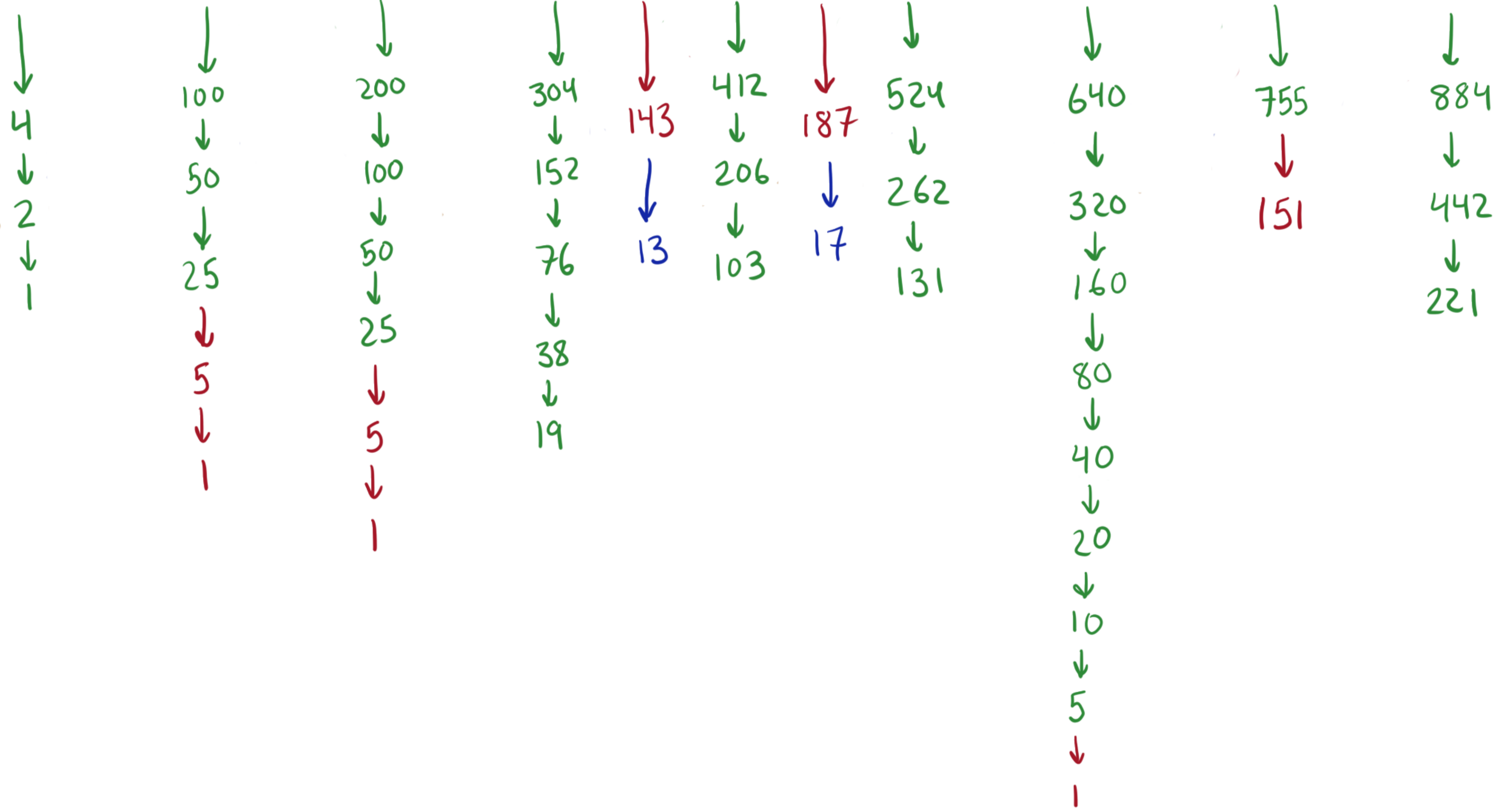
$k \pmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \pmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \pmod{11}$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \pmod{13}$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11

$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768



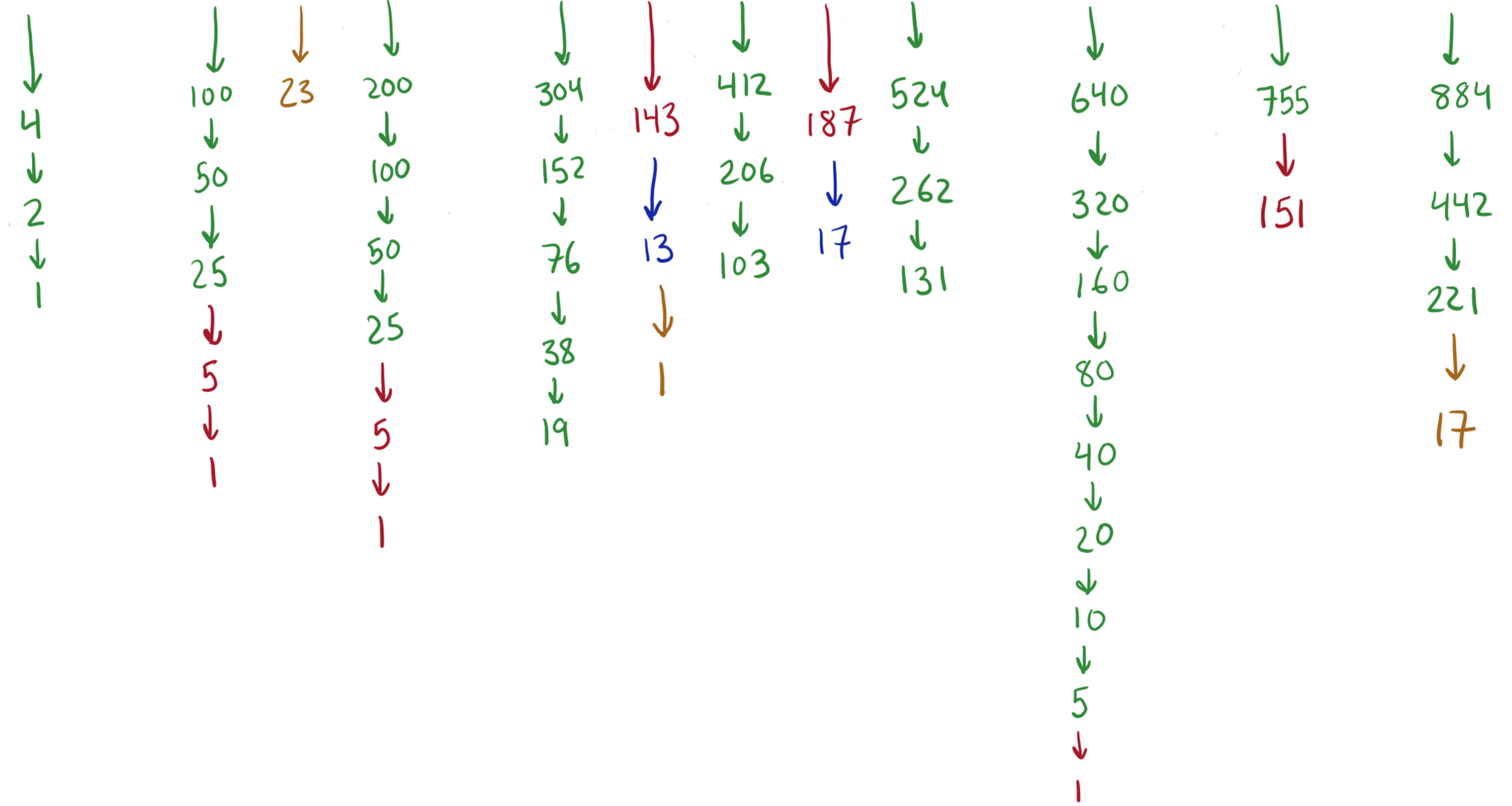
$k \pmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \pmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \pmod{11}$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \pmod{13}$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11

$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768



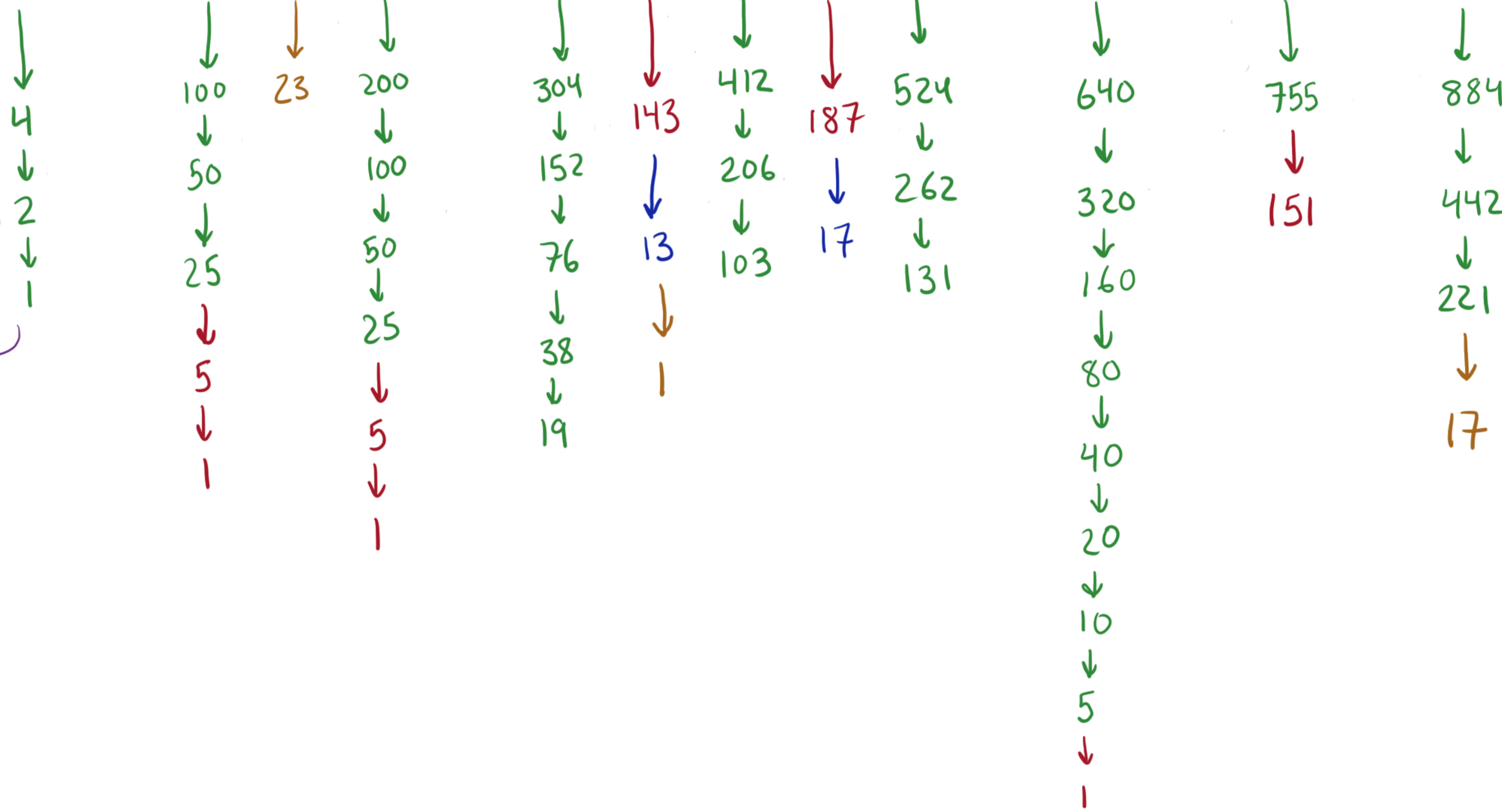
$k \pmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \pmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \pmod{11}$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \pmod{13}$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11

$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768



$k \pmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \pmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \pmod{11}$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \pmod{13}$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11

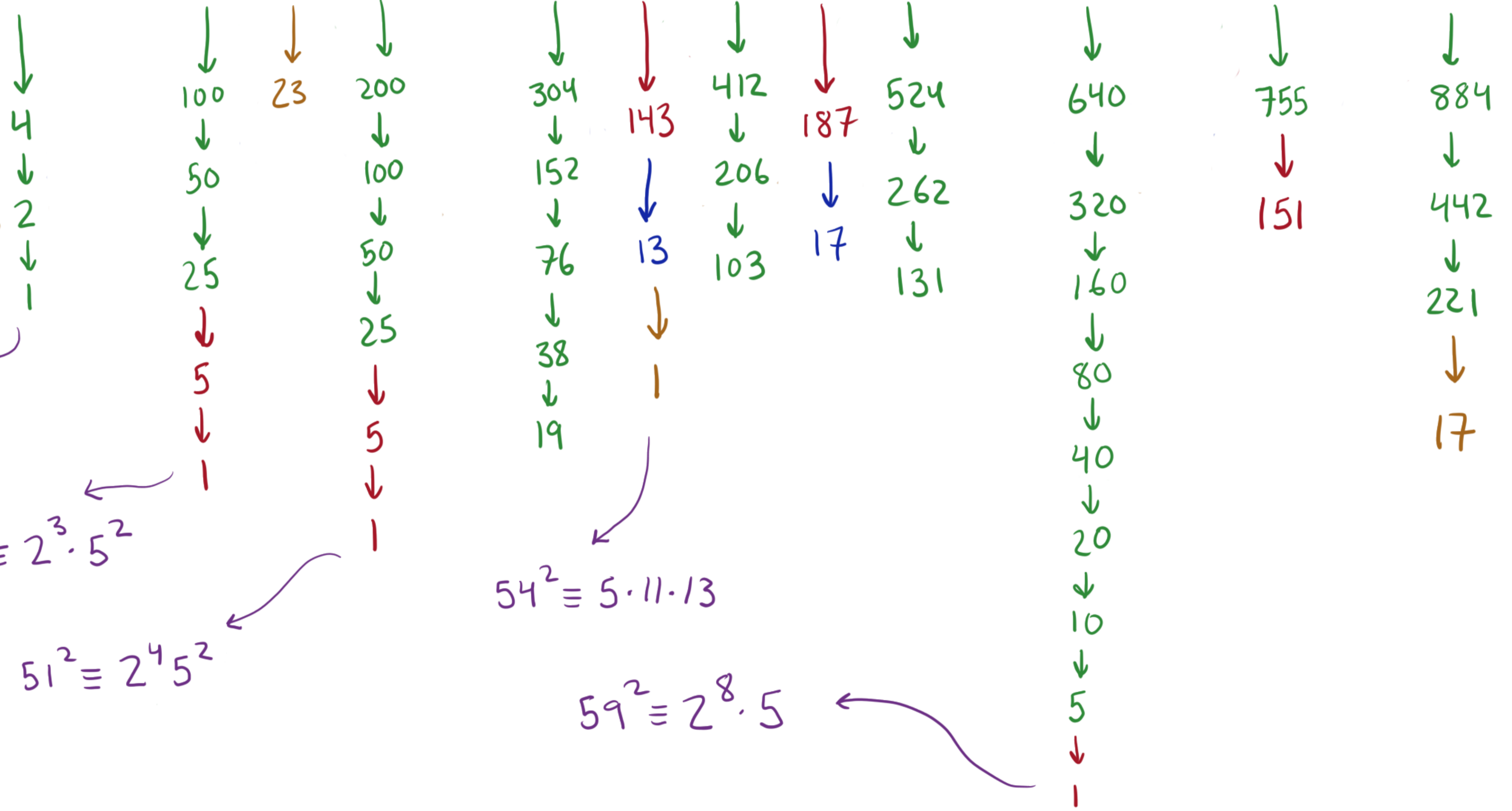
$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768



$47^2 \equiv 2^3$

$k \pmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \pmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \pmod{11}$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \pmod{13}$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11

$k$	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$k^2 - n$	8	103	200	299	400	503	608	715	824	935	1048	1163	1280	1399	1520	1643	1768



$47^2 \equiv 2^3$

$49^2 \equiv 2^3 \cdot 5^2$

$51^2 \equiv 2^4 \cdot 5^2$

$54^2 \equiv 5 \cdot 11 \cdot 13$

$59^2 \equiv 2^8 \cdot 5$