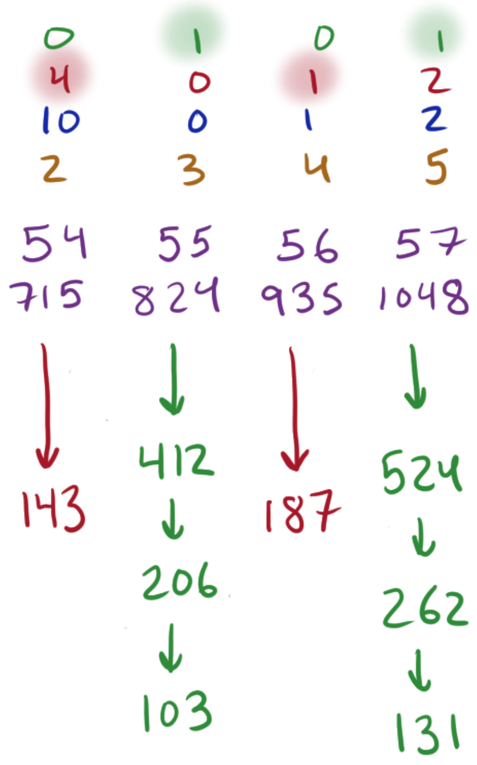
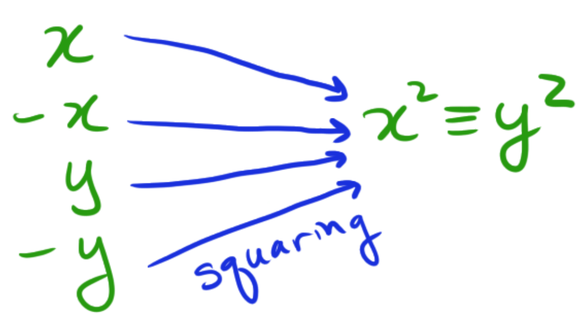
Quadratic Sieve Factoring: Visually



Proof of Concept

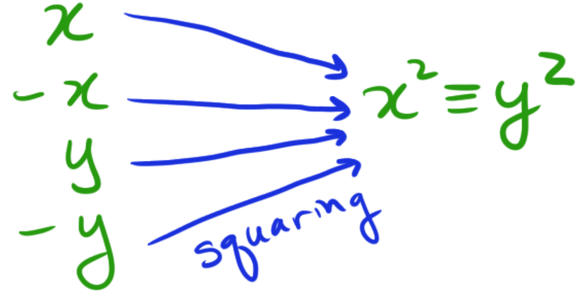
A surfeit of square roots

If $x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv \pm y \pmod{n}$, then we have a surfeit of square roots:



A surfeit of square roots

If $x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv \pm y \pmod{n}$, then we have a surfeit of square roots:



$$x^2 \equiv y^2 \pmod{n}$$

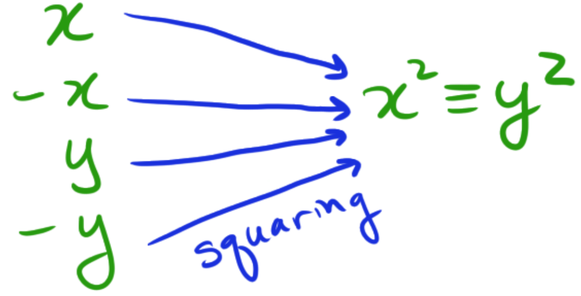
$$n \mid (x+y)(x-y)$$

$$x \not\equiv \pm y \pmod{n}$$

$$n \nmid x+y$$
$$n \nmid x-y$$

A surfeit of square roots

If $x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv \pm y \pmod{n}$, then we have a surfeit of square roots:



$$x^2 \equiv y^2 \pmod{n}$$

$$n \mid (x+y)(x-y)$$

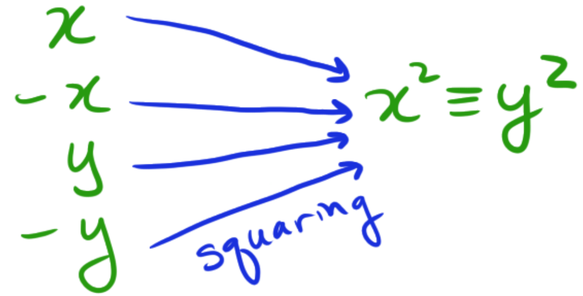
must each contain "part" (not all) of n

$$x \not\equiv \pm y \pmod{n}$$

$$n \nmid x+y$$
$$n \nmid x-y$$

A surfeit of square roots

If $x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv \pm y \pmod{n}$, then we have a surfeit of square roots:



So gcd(x+y, n) should be a non-trivial factor of n

$$x^2 \equiv y^2 \pmod{n}$$

$$n \mid (x+y)(x-y)$$

must each contain "part" (not all) of n

$$x \not\equiv \pm y \pmod{n}$$

$$n \nmid x+y$$
$$n \nmid x-y$$

$$n = 3 \cdot 13$$

$$= (x-y)(x+y) \quad \text{when} \quad \begin{matrix} x = 8 \\ y = 5 \end{matrix}$$

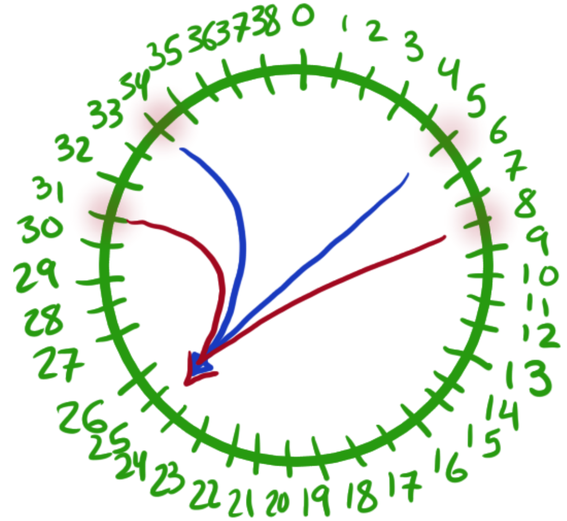
$$n = 3 \cdot 13 = 39$$

$$= (x-y)(x+y) \quad \text{when} \quad \begin{matrix} x = 8 \\ y = 5 \end{matrix}$$

mod n : $8^2 \equiv 25$

$5^2 \equiv 25$

but $8 \not\equiv \pm 5$



Goal: Find $x^2 \equiv y^2 \pmod{n}$ with $x \not\equiv \pm y \pmod{n}$.

Goal: Find $x^2 \equiv y^2 \pmod{n}$ with $x \not\equiv \pm y \pmod{n}$.

Payoff: Take $\gcd(x-y, n)$ to find a non-trivial factor of n.

Goal: Find $x^2 \equiv y^2 \pmod{n}$ with $x \not\equiv \pm y \pmod{n}$.

Payoff: Take $\gcd(x-y, n)$ to find a non-trivial factor of n.

Strategy: Look for $k^2 - n = \square$

Example.

$n = 39 = 3 \cdot 13$

$7^2 - n = 49 - 39 = 10$ ← not a square ☹

$8^2 - n = 64 - 39 = 25$ ← a square! ☺

$= 5^2$

So $8^2 \equiv 5^2 \pmod{n}$

Problem: This is very unlikely!

Example.

$n = 39 = 3 \cdot 13$

$7^2 - n = 49 - 39 = 10 = 2 \cdot 5$

$8^2 - n = 64 - 39 = 25 = 5^2$

$9^2 - n = 81 - 39 = 42 = 2 \cdot 3 \cdot 7$

$10^2 - n = 100 - 39 = 61 = 61$

$11^2 - n = 121 - 39 = 82 = 2 \cdot 41$

$12^2 - n = 144 - 39 = 105 = 3 \cdot 5 \cdot 7$

$13^2 - n = 169 - 39 = 130 = 2 \cdot 5 \cdot 13$

mod n

$7^2 \cdot 9^2 \cdot 12^2$

$\equiv 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2$

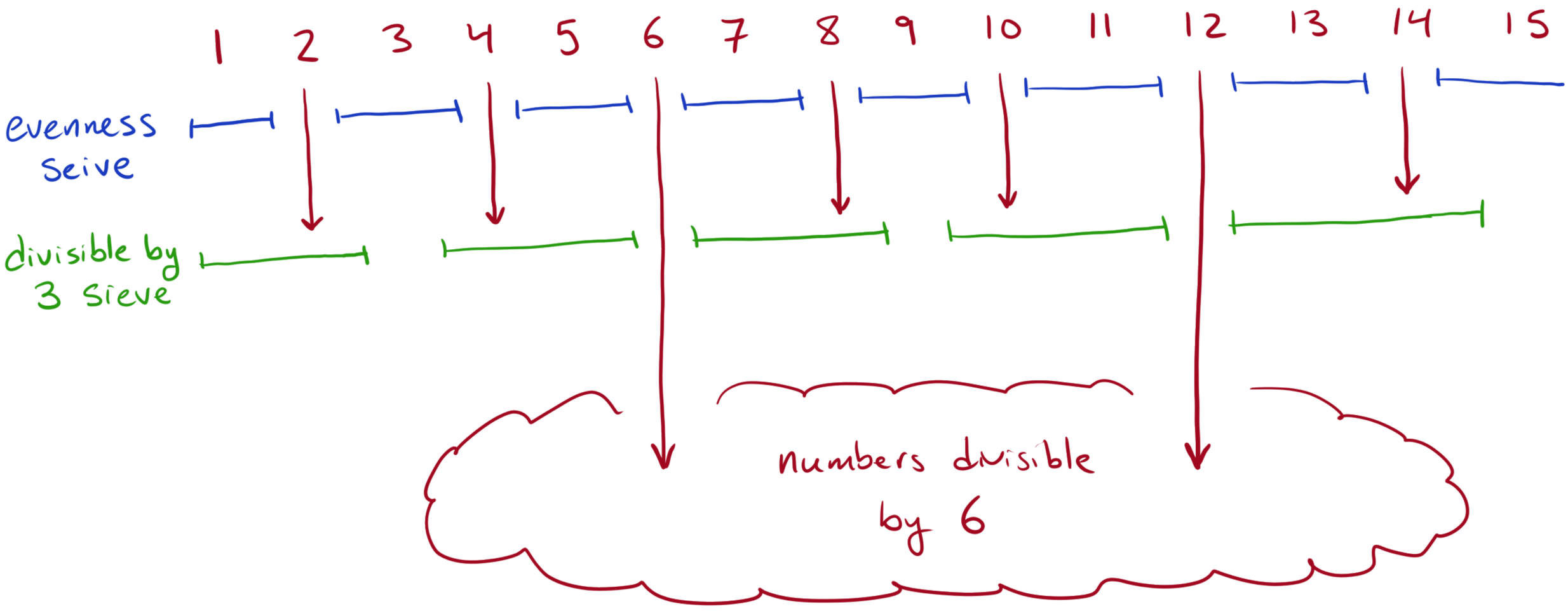
$x^2 \equiv y^2$



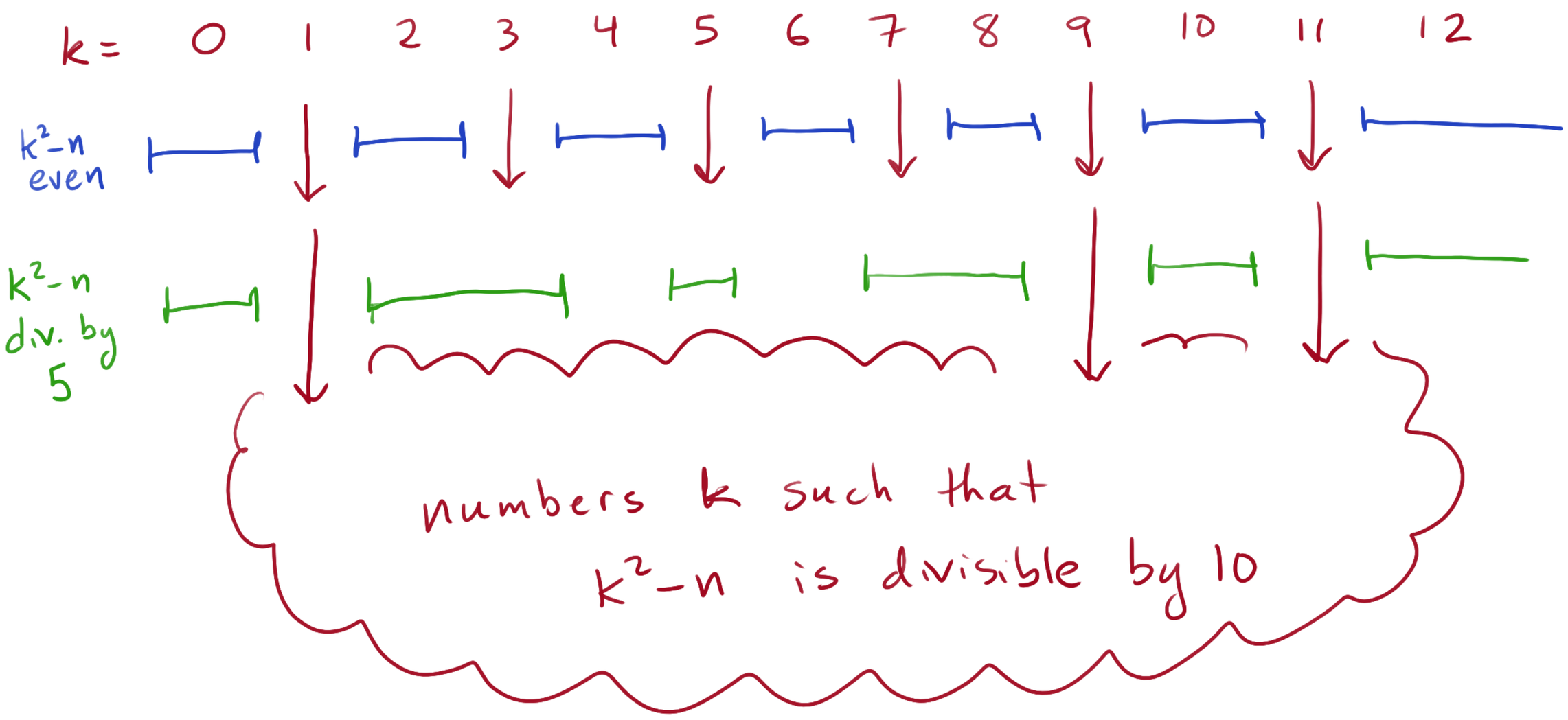
Core Idea: Factor $k^2 - n$ for various k

Look for combinations to form $x^2 \equiv y^2$

Sieving

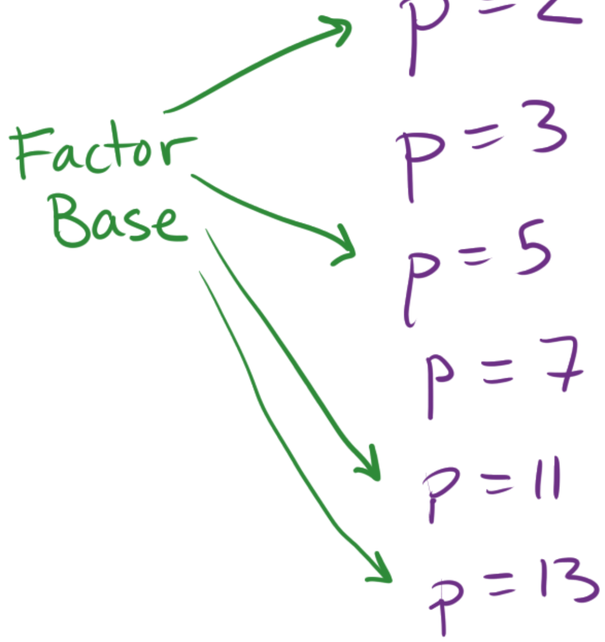

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
evenness sieve
divisible by 3 sieve
numbers divisible by 6

Sieving k^2-n


k = 0 1 2 3 4 5 6 7 8 9 10 11 12
k²-n even
k²-n div. by 5
numbers k such that
k²-n is divisible by 10

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

$$n = 2201$$



prime	equation	solutions
$p=2$	$x^2 \equiv n \pmod 2$	$x \equiv 1$
$p=3$	$x^2 \equiv n \pmod 3$	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

$n = 2201$ $\quad \sqrt{n} \approx 47$

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

$$\Downarrow$$

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

$k \bmod 2$	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

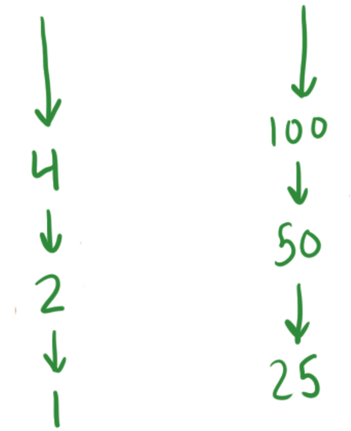


4

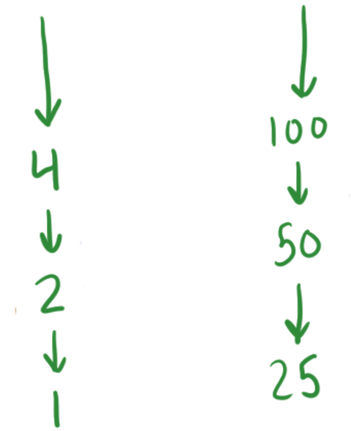
$k \bmod 2$	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$k \bmod 5$	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
$k \bmod 11$	3	4	5	6	7	8	9	10	0	1	2	3	4	5	6	7	8
$k \bmod 13$	8	9	10	11	12	0	1	2	3	4	5	6	7	8	9	10	11
k	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
k^2-n	8	103	200	299	400	503	608	715	824	935	1048	1163	1280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



$k \bmod 2$	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



$k \bmod 2$	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

8 → 4 → 2 → 1

200 → 100 → 50 → 25

400 → 200 → 100 → 50 → 25

608 → 304 → 152 → 76 → 38 → 19

824 → 412 → 206 → 103

1048 → 524 → 262 → 131

1280 → 640 → 320 → 160 → 80 → 40 → 20 → 10 → 5

1520 → 755

1768 → 884 → 442 → 221

$k \bmod 2$	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

47: 8 → 4 → 2 → 1

49: 200 → 100 → 50 → 25

51: 400 → 200 → 100 → 50 → 25

53: 608 → 304 → 152 → 76 → 38 → 19

54: 715 → 143

55: 824 → 412 → 206 → 103

56: 935 → 187

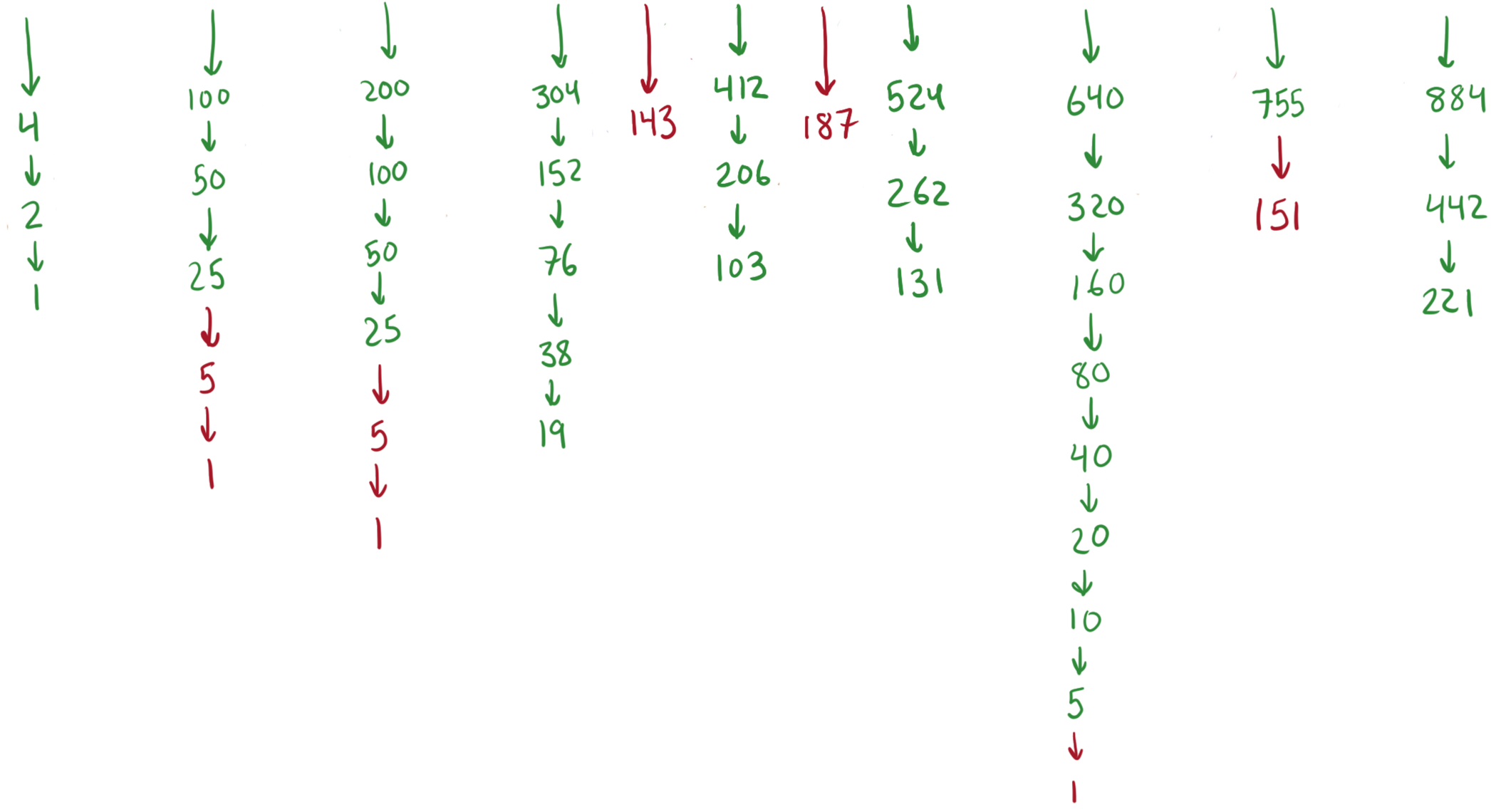
57: 1048 → 524 → 262 → 131

59: 1280 → 640 → 320 → 160 → 80 → 40 → 20 → 10 → 5

61: 1520 → 755

63: 1768 → 884 → 442 → 221

$k \bmod 2$	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

8 → 4 → 2 → 1

200 → 100 → 50 → 25 → 5 → 1

400 → 200 → 100 → 50 → 25 → 5 → 1

608 → 304 → 152 → 76 → 38 → 19

715 → 143

824 → 412 → 206 → 103

935 → 187

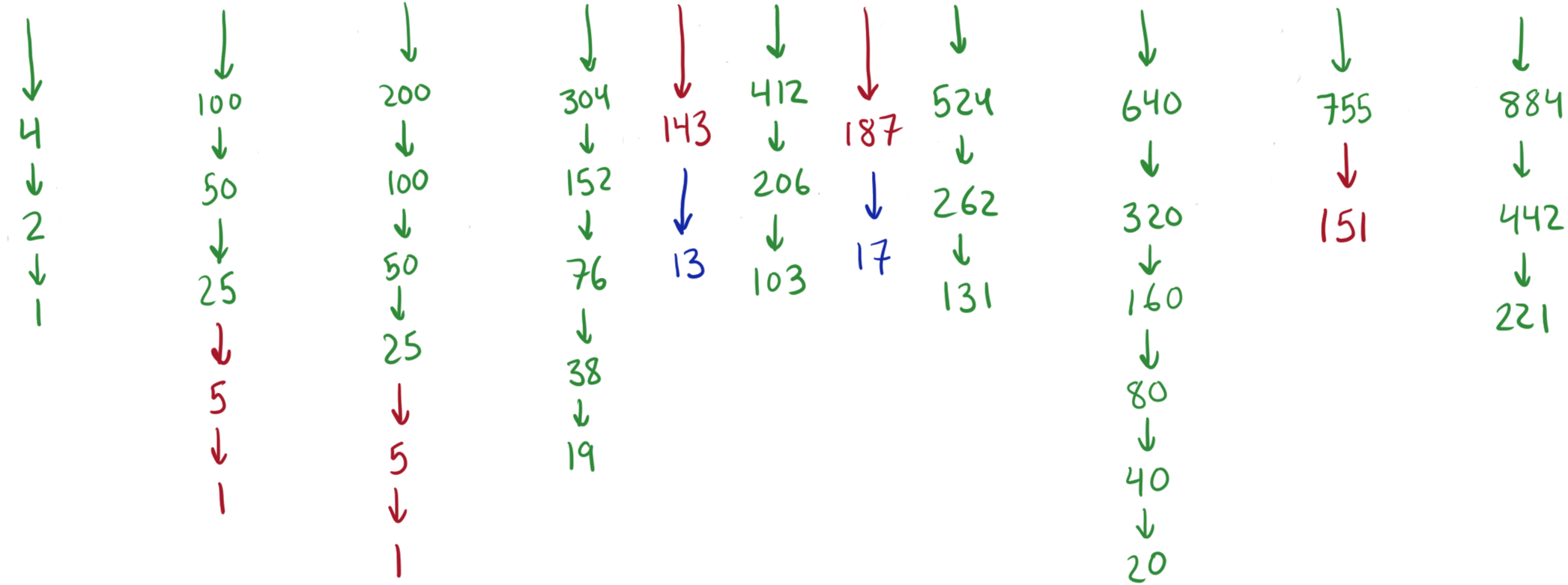
1048 → 524 → 262 → 131

1280 → 640 → 320 → 160 → 80 → 40 → 20 → 10 → 5 → 1

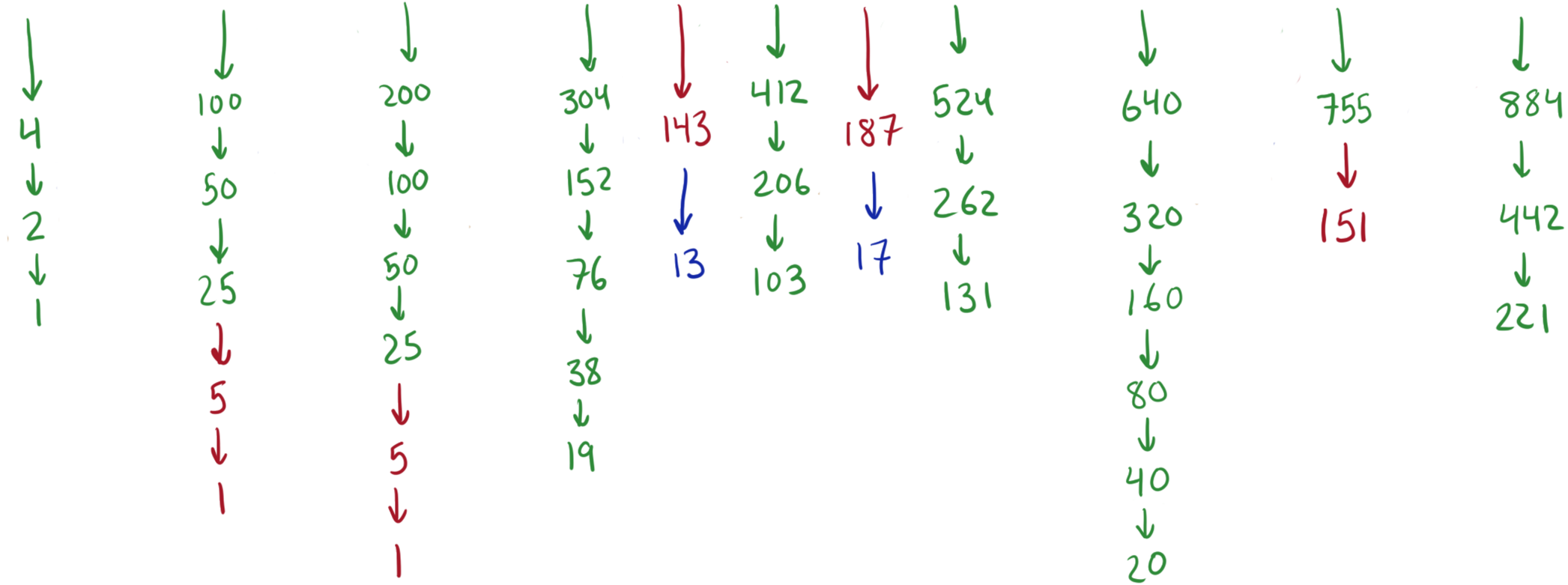
1520 → 755 → 151

1768 → 884 → 442 → 221

$k \bmod 2$	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



$k \bmod 2$	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

47: 8 → 4 → 2 → 1

$47^2 \equiv 2^3$

49: 200 → 100 → 50 → 25 → 5 → 1

50: 299 → 23

51: 400 → 200 → 100 → 50 → 25 → 5 → 1

53: 608 → 304 → 152 → 76 → 38 → 19

54: 715 → 143 → 13 → 1

55: 824 → 412 → 206 → 103

56: 935 → 187 → 17

57: 1048 → 524 → 262 → 131

59: 1280 → 640 → 320 → 160 → 80 → 40 → 20 → 10 → 5 → 1

61: 1520 → 755 → 151

63: 1768 → 884 → 442 → 221 → 17

$k \bmod 2$	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

$47^2 \equiv 2^3$

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

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

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

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

$k \bmod 2$	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

47 → 4 → 2 → 1

$47^2 \equiv 2^3$

49 → 100 → 50 → 25 → 5 → 1

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

51 → 200 → 100 → 50 → 25 → 5 → 1

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

23

54 → 304 → 152 → 76 → 38 → 19

143 → 13 → 1

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

55 → 412 → 206 → 103

56 → 187 → 17

57 → 524 → 262 → 131

59 → 640 → 320 → 160 → 80 → 40 → 20 → 10 → 5 → 1

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

61 → 755 → 151

63 → 884 → 442 → 221 → 17

$$(47 \cdot 49)^2 \equiv (2^3 \cdot 5)^2 \mod n$$

$$102^2 \equiv 40^2 \mod 2201$$

$47^2 \equiv 2^3$

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

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

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

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

$$(47 \cdot 49)^2 \equiv (2^3 \cdot 5)^2 \mod n$$

$$102^2 \equiv 40^2 \mod 2201$$

$47^2 \equiv 2^3$

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

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

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

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

$\gcd(102-40, 2201)$

$= 31$

$2201 = 31 \cdot 71$

Summary:

1) Choose $k_0 \sim \sqrt{n}$

2) Choose factor base: $p_1, p_2, \ldots$ such that $x^2 \equiv n \pmod{p_i}$ has solutions

3) Solve $x^2 \equiv n \pmod{p_i}$ each p_i to create a sieve.

4) For $k = k_0, k_0+1, k_0+2$, etc. apply the sieve

   ↳ Obtain $k^2 - n =$ product of p_i's } relations

5) Combine relations to obtain

$$k^2 - n = y^2 \quad \Rightarrow \quad n = k^2 - y^2 = (k+y)(k-y)$$

need $y \not\equiv \pm k \pmod{n}$