트위터의 타임라인을 보다보니 다항식 $x^2 - 2999x + 2248541$이 $1460 \le x \le 1539$ 일 때, 소수가 된다는 트윗이 보인다. 왜 그런지 한번 생각해 보자.

-163과 오일러의 소수 생성 다항식 $x^2 + x + 41$

$x^2 - 2999x + 2248541$는 이차다항식이므로 판별식을 한번 계산해 보자.

```
Discriminant[x^2 - 2999 x + 2248541, x]
```

```
-163
```

-163 이라는 숫자가 나왔다. 정수론에 관심이 있는 사람이라면 여기서 뭔가를 느낄 수 있다. 왜냐하면 이는 바로 오일러의 소수 생성 다항식 $x^2 + x + 41$ 의 판별식이기 때문이다.

```
Discriminant[x^2 + x + 41, x]
```

```
-163
```

아마도 위의 다항식은 오일러의 소수 생성 다항식을 약간 숨겨 놓은 것에 불과할 것이라고 추측된다. $x^2 - 2999x + 2248541$에 있는 x의 자리에 $x + 1500$ 을 넣고 정리를 해보자.

```
Expand[x^2 - 2999 x + 2248541 /. {x → x + 1500}]
```

```
41 + x + x^2
```

결국 맨 위에 있는 말은 "오일러의 소수 생성 다항식 $x^2 + x + 41$은 $-40 \le x \le 39$ 인 정수 x에 대하여 소수가 된다" 는 사실을 살짝 꼬아놓은 것에 불과하다.

소수판정

$-40 \le x \le 39$일 때, $f(x) = x^2 + x + 41$의 값을 한번 살펴 보자.

```
f[x_] := x^2 + x + 41
Table[f[x], {x, -40, 39}]
```

```
{1601, 1523, 1447, 1373, 1301, 1231, 1163, 1097, 1033, 971, 911, 853, 797, 743,
 691, 641, 593, 547, 503, 461, 421, 383, 347, 313, 281, 251, 223, 197, 173, 151,
 131, 113, 97, 83, 71, 61, 53, 47, 43, 41, 41, 43, 47, 53, 61, 71, 83, 97, 113, 131,
 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691,
 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601}
```

이 테이블을 보면, $f(-40) = f(39)$, $f(-39) = f(38), \cdots, f(-1) = f(0)$ 임을 관찰할 수 있다. $f(-x-1) = f(x)$ 이 성립하기 때문이다.

```
Simplify[f[-x - 1] - f[x]]
```

```
0
```

$-40 \le x \le 39$일 때를 생각하는 대신 , $0 \le x \le 39$ 일 때, $f(x) = x^2 + x + 41$의 값이 소수가 됨을 보여도 충분함을 알게 되었다. 그럼 테이블을 만들어 보자.

```
X := Table[x, {x, 0, 39}]
T := Table[{f[x]}, {x, X}]
TableForm[T, TableHeadings → {X, {"x^2+x+41"}}]
```

	x^2+x+41
0	41
1	43
2	47
3	53
4	61
5	71
6	83
7	97
8	113
9	131
10	151
11	173
12	197
13	223
14	251
15	281
16	313
17	347
18	383
19	421
20	461
21	503
22	547
23	593
24	641
25	691
26	743
27	797
28	853
29	911
30	971
31	1033
32	1097
33	1163
34	1231
35	1301
36	1373
37	1447
38	1523
39	1601

이제 이 테이블을 가지고 이들이 정말 모두 소수가 되는지 생각해 보자.

자연수 n이 주어져 있을 때, n이 소수인지 아닌지를 알려면 $\sqrt{n}$ 보다 작은 모든

소수로 나눠보아 나누어지지 않음을 확인하면 된다.

작은 소수에 대해서부터 따져보자. 2로 나눈 나머지를 보자.

```
M[p_] := Table[{f[x], Mod[f[x], p]}, {x, X}]
TableForm[M[2], TableHeadings → {X, {"x^2+x+41", "mod 2"}}]
```

	x^2+x+41	mod 2
0	41	1
1	43	1
2	47	1
3	53	1
4	61	1
5	71	1
6	83	1
7	97	1
8	113	1
9	131	1
10	151	1
11	173	1
12	197	1
13	223	1
14	251	1
15	281	1
16	313	1
17	347	1
18	383	1
19	421	1
20	461	1
21	503	1
22	547	1
23	593	1
24	641	1
25	691	1
26	743	1
27	797	1
28	853	1
29	911	1
30	971	1
31	1033	1
32	1097	1
33	1163	1
34	1231	1
35	1301	1
36	1373	1
37	1447	1
38	1523	1
39	1601	1

모두 1이 된다. 이는 위의 테이블에 있는 40개의 숫자들이 모두 홀수가 됨을 보여준다. 따라서 2로는

나누어지지 않음을 확인할 수 있다.
이제 그 다음 소수인 3으로 나눈 나머지도 따져보자.

```
TableForm[M[3], TableHeadings → {X, {"x^2+x+41", "mod 3"}}]
```

	x^2+x+41	mod 3
0	41	2
1	43	1
2	47	2
3	53	2
4	61	1
5	71	2
6	83	2
7	97	1
8	113	2
9	131	2
10	151	1
11	173	2
12	197	2
13	223	1
14	251	2
15	281	2
16	313	1
17	347	2
18	383	2
19	421	1
20	461	2
21	503	2
22	547	1
23	593	2
24	641	2
25	691	1
26	743	2
27	797	2
28	853	1
29	911	2
30	971	2
31	1033	1
32	1097	2
33	1163	2
34	1231	1
35	1301	2
36	1373	2
37	1447	1
38	1523	2
39	1601	2

3으로 나누어지지 않음을 확인했다. 5에 대해서도 한번 해보자.

```
TableForm[M[5], TableHeadings → {X, {"x^2+x+41", "mod 5"}}]
```

	x^2+x+41	mod 5
0	41	1
1	43	3
2	47	2
3	53	3
4	61	1
5	71	1
6	83	3
7	97	2
8	113	3
9	131	1
10	151	1
11	173	3
12	197	2
13	223	3
14	251	1
15	281	1
16	313	3
17	347	2
18	383	3
19	421	1
20	461	1
21	503	3
22	547	2
23	593	3
24	641	1
25	691	1
26	743	3
27	797	2
28	853	3
29	911	1
30	971	1
31	1033	3
32	1097	2
33	1163	3
34	1231	1
35	1301	1
36	1373	3
37	1447	2
38	1523	3
39	1601	1

이들은 모두 5로도 나누어지지 않는다.

이렇게 하나하나의 소수에 대하여 테스트를 한다고 할때, 어느 소수까지 테스트를 해 보면 충분할까? n이 소수인지 아닌지를 알려면 $\sqrt{n}$ 보다 작은 모든 소수로 나눠보아 나누어지지 않음을 확인하면 되므로

$\sqrt{1601} \approx 40$보다 작은 소수들에 대해 따져보면 충분하다.

```
N[Sqrt[1601], 10]
```

```
40.01249805
```

15개 정도의 소수의 목록을 뽑아보면,

```
Table[Prime[n], {n, 1, 15}]
```

```
{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47}
```

한번 위의 5로 나눈 나머지의 표를 가만 보면 1,3,2,3,1 가 계속해서 반복된다는 것을 관찰할 수 있다. 이 주기성은 합동식의 성질을 생각하면 쉽게 알 수 있는 것이다. 따라서 40개의 숫자의 나머지를 모두 체크하는 것은 불필요한 일이다. 5에 대한 나머지를 따지는 것으로 것이라면, $0 \le x \le 4$ 일 때의 $x^2 + x + 41$값의 나머지만 따져보면 되는 것이다.

정리하자면, 2부터 37 사이에 있는 12개의 소수 p에 대해서 $0 \le x \le p - 1$ 일 때 $x^2 + x + 41$의 p로 나눈 나머지가 0이 되지 않는다는 것을 보이면 원하는 것이 증명된다. 여기서 이차잉여의 개념이 등장하게 된다.

이차잉여의 등장

소수 p를 하나 고정시키자. $0 \le x \le p - 1$일 때, $x^2 + x + 41$의 p로 나눈 나머지가 0이 되지 않는다는 것을 증명하기 위해 다항식 $f(x) = x^2 + x + 41$를 mod p로 따져보자.
$p = 2$인 경우는

```
PolynomialMod[f[x], 2]
```

```
1 + x + x^2
```

$x^2 + x + 41 \equiv x^2 + x + 1 \equiv x(x+1) + 1 \pmod 2$이므로 어떤 정수 x에 대해서도 $x^2 + x + 41$를 2로 나눈 나머지가 0이 되지 않음을 증명할 수 있다.

$p = 3$인 경우는

```
PolynomialMod[f[x], 3]
```

```
2 + x + x^2
```

mod 3 으로 생각할 때, $x^2 + x + 41 \equiv x^2 + x + 2 \equiv (x+2)^2 + 1 \pmod 3$ 이 성립한다.

```
PolynomialMod[(x + 2)^2 + 1, 3]
```

```
2 + x + x^2
```

그러나 $(x+2)^2+1 \pmod 3$ 은 절대로 0이 될 수 없는데, 이는 $-1 \equiv 2$이 3의 비이차잉여, 즉 합동식 $y^2 \equiv -1 \pmod 3$ 를 만족시키는 y는 존재하지 않기 때문이다.

mod 5 로 생각한다면,

```
PolynomialMod[f[x], 5]
```

```
1 + x + x^2
```

이를 위에서처럼 완전제곱꼴로 표현해보자. $x^2+x+1 \equiv (x+3)^2-9+1 \equiv (x+3)^2+2 \pmod 5$ 이 성립한다.

```
PolynomialMod[(x + 3)^2 + 2, 5]
```

```
1 + x + x^2
```

$(x+3)^2+2 \pmod 5$ 는 절대로 0이 될 수 없는데, 이는 $-2 \equiv 3$이 5의 비이차잉여, 즉 합동식 $y^2 \equiv 3 \pmod 5$ 를 만족시키는 y는 존재하지 않기 때문이다. 이제 일반적인 증명이 가능하다.

증명 : 소수 $2 \le p \le 37$ 에 대하여, x^2+x+41의 p로 나눈 나머지는 0이 될 수 없다.

$p=2$ 인 경우는 위에서 증명하였다.
소수 $2 < p \le 37$ 를 하나 고정시키자. $\{1, 2, \cdots, p-1\}$는 기약잉여계이므로, $2b \equiv 1 \pmod p$ 를 만족시키는 b는 반드시 존재한다.
$x^2+x+41 \equiv (x+b)^2-b^2+41 \pmod p$ 이므로, 만약에 b^2-41이 소수 p에 대한 비이차잉여임을 보이면 충분하다. 르장드르 부호를 계산해보자.

$$\left(\frac{b^2-41}{p}\right) = \left(\frac{2^2}{p}\right)\left(\frac{b^2-41}{p}\right) = \left(\frac{(2b)^2-164}{p}\right) = \left(\frac{-163}{p}\right)$$

-163 !!!

마침내 -163이 등장했다. 소수 $2 < p \le 37$ 가 모두 $\left(\frac{-163}{p}\right) = -1$ 를 만족시키는 보이는 것으로 충분하다.

```
Table[{Prime[n], JacobiSymbol[-163, Prime[n]]}, {n, 2, 12}] // TableForm
```

```
3     -1
5     -1
7     -1
11    -1
13    -1
17    -1
19    -1
23    -1
29    -1
31    -1
37    -1
```

이렇게 하여 "오일러의 소수 생성 다항식 $x^2 + x + 41$은 $-40 \le x \le 39$ 인 정수 x에 대하여 소수가 된다"는 것을 알 수 있다.