

The following is a special case of Dirichlet's Theorem.

**Proposition 1.** (*Proposition 3.38 in Erickson/Vazzana*).

*There are infinitely many primes of the form  $4k + 1$ .*

**Remark:** The case  $4k + 3$  is Proposition 2.38.

*Proof.* Let  $N \geq 2$ . None of the numbers  $2, 3, 4, \dots, N$  divide  $P = (2 \cdot 3 \cdot 4 \cdot \dots \cdot N)^2 + 1$ . Then for any prime factor  $p$  of  $P$  we have  $p > N$ . Now

$$p \mid (N!)^2 + 1 \Leftrightarrow (N!)^2 \equiv -1 \pmod{p}$$

so  $x = N!$  is a solution to the quadratic congruence

$$x^2 \equiv -1 \pmod{p}.$$

But by Theorem 3.37 this congruence only has solutions if  $p = 2$  or  $p = 4k + 1$ . Since  $p > N \geq 2$ , we have  $p = 4k + 1$ . So for any  $N$  there exists a prime  $p$  with  $p > N$  and  $p = 4k + 1$ . Hence there are infinitely many primes of the form  $4k + 1$ .  $\square$

**Remark:** The first steps are

$$2^2 + 1 = 5$$

$$(3!)^2 + 1 = 37$$

$$(4!)^2 + 1 = 577$$

$$(5!)^2 + 1 = 14401$$

$$(6!)^2 + 1 = 518401 = 13 \cdot 39877.$$