$a^n \pm 1$ and exponent lifting

1. (Revision) Prove that there are infinitely many primes of the form $4m+1$.
2. (Revision) Determine whether there exist rational numbers r and q such that $r^2+q^2=38$.

Definition 1. *For a prime number p and a nonnegative integer k, write $p^k \mid\mid n$ to mean that $p^k \mid n$ and $p^{k+1} \nmid n$.*

In the case we will say that n is exactly (or fully) divisible by p^k. For example, $5^2 \mid\mid 50$. It means the same as $\nu_5(50)=2$.

Lemma 1 (Exponent lifting). *Let $a \geqslant 2$, $k \geqslant 1$, $l \geqslant 0$ be integers, and p be a prime number. Suppose $(p,k) \neq (2,1)$ and*

$$p^k \mid\mid a-1, \qquad p^l \mid\mid n.$$

Then

$$p^{k+l} \mid\mid a^n-1.$$

The same fact can be presented as

$$\nu_p(a^n-1)=\nu_p(a-1)+\nu_p(n).$$

For example,

$$\nu_3(14^{18}-2^{18})=\nu_3(14-2)+\nu_3(18)=1+2=3$$

3. Let k be a nonnegative integer. Using exponent lifting lemma, prove that $3^{k+1} \mid\mid 2^{3^k}+1$.
4. Prove Lemma 1.

Definition 2. *Recall that a* **primitive root** $\pmod n$ *is a number g such that the smallest positive integer k for which $g^k \equiv 1 \pmod n$ is $\varphi(n)$.*

5. Show that 2 is a primitive root $\pmod{3^n}$ for any $n \in \mathbb{N}$.
6. Show that if $p>2$ is a prime, g is a primitive root $\pmod p$, and $p^2 \nmid g^{p-1}-1$, then g is a primitive root $\pmod{p^n}$ for any $n \in \mathbb{N}$.
7. Find the smallest positive integer n such that 3^n ends with 01 when written in base 143.
8. (USA TST) Prove that n^7+7 is not a perfect square for any positive integer n.
9. Find all primes $p>2$ and positive integers (x,y) such that $x^{p-1}+y$ and $y^{p-1}+x$ are powers of p.

$a^n \pm 1$ and exponent lifting (homework)

10. Show that if $p>2$ is a prime, g is an odd primitive root $\pmod p$, and $p^2 \nmid g^{p-1}-1$, then g is a primitive root $\pmod{2p^n}$ for any $n \in \mathbb{N}$.
11. Let n be a square-free integer (that is n is not divisible by any perfect square $b^2>1$). Find all pairs of coprime positive integers (x,y) such that x^n+y^n is divisible by $(x+y)^3$.
12. (Exponent lifting lemma - generalization) Let a and b be an integers and p a prime. Assume that

    (а) $p \mid (a-b)$

    (б) $p \nmid a$ and $p \nmid b$

    (в) $p>2$.

    Then

$$\nu_p(a^n-b^n)=\nu_p(a-b)+\nu_p(n).$$