Primes - Problem Sheet 2

Elementary proofs for Fermat's claims

Setup

Q1) Find a generalisation of the identity

$$(x^2+y^2)(z^2+w^2) = (xz \pm yw)^2 + (xw \mp yz)^2$$

to

$$(x^2+ny^2)(z^2+nw^2) = (\cdots)^2 + n(\cdots)^2\,,$$

and

$$(ax^2+cy^2)(az^2+cw^2) = (\cdots)^2 + ac(\cdots)^2\,.$$

Recall the following lemma

Lemma 1. *Suppose $N = a^2+b^2$ is a sum of two relative prime squares* $\gcd(a,b)=1$. *If $q = x^2+y^2$ is a prime divisor of N, then N/q is also a sum of two relatively prime squares.*

Q2) Formulate a version of the above lemma when a prime $q = x^2+ny^2$ divides $N = a^2+nb^2$, with n a positive integer. Show also the statement holds when $q = 4$ and $n = 3$.

Q3) Suppose a prime p divides $N = a^2+nb^2$, $\gcd(a,b)=1$. Is it true that $p = x^2+ny^2$, for some $\gcd(x,y)=1$? Give a proof or a counterexample. What does this say about our ability to complete the *Descent* step in general?

Fermat's x^2+2y^2 claim

In the following exercises you will prove Fermat's theorem for primes $p = x^2+2y^2$.

Q4) Suppose that prime $p = x^2+2y^2$. By reducing modulo 8, show that $p = 2$ or $p \equiv 1, 3 \pmod 8$.

Q5) (Descent for x^2+2y^2) Suppose prime p divides x^2+2y^2, with $\gcd(x,y)=1$. Adapt the proof of Fermat's two-squares theorem (Theorem 2.4) to show that $p = a^2+2b^2$. Hint: Q2) might be useful.

Q6) (Reciprocity for x^2+2y^2) Suppose prime $p \equiv 1, 3 \pmod 8$. Show that $p \mid x^2+2y^2$, for some $\gcd(x,y)=1$, by completing the following steps.

i) For $p \equiv 1 \pmod 8$, make use of the identity:

$$x^{8k}-1 = (x^{4k}-1)[(x^{2k}-1)^2+2x^{2k}]$$

ii) For $p \equiv 3 \pmod 8$, argue as follows.

a) (Optional) Show descent works for x^2-2y^2.

b) Use descent for x^2-2y^2, to show p does not divide any $N = x^2-2y^2$. Conclude that $2 \not\equiv a^2 \pmod p$.

c) Show p does not divide any $N = x^2+y^2$.

d) Write $p = 2m+1$, and show that no two of the following are congruence, modulo p

$$1^2, 2^2, \ldots, m^2, -1^2, -2^2, \ldots, -m^2 .$$

Hence conclude exactly one of $-a$ and a is a square, modulo p. In particular, show -2 is a square, modulo p.

e) Show that $p \mid x^2 + 2y^2$, with some $\gcd(x, y) = 1$. (Take $x = 1$.)

f) (Optional/research) Is it possible to more directly show $p \equiv 3 \pmod 8$ divides some x^2+2y^2, $\gcd(x, y) = 1$? For example, by using a polynomial identity like above?

Conclude that Fermat's claim about $p = x^2 + 2y^2$ holds.

Q7) Find (with proof!) a condition on when a positive integer N can be written in the form $N = x^2 + 2y^2$, $x, y \in \mathbb{Z}$.

Fermat's $x^2 + 3y^2$ claim

In the following exercises you will prove Fermat's theorem for primes $p = x^2 + 3y^2$.

Q8) Suppose that prime $p = x^2 + 3y^2$. By reducing modulo 3, show that $p = 3$, or $p \equiv 1 \pmod 3$.

Q9) (Descent for $x^2 + 3y^2$) Suppose prime p divides $x^2 + 3y^2$, with $\gcd(x, y) = 1$. Show that $p = a^2 + 3b^2$. Warning: the descent step doesn't work for $p = 2$, so if $p \neq a^2 + 3b^2$ you need to produce an *odd* prime $q < p$ not of this form.

Q10) (Reciprocity for x^2+3y^2) Suppose prime $p \equiv 1 \pmod 3$. Show that $p \mid x^2+3y^2$, for some $\gcd(x, y) = 1$. Hint:

$$4(x^{3k} - 1) = (x^k - 1)[(2x^k + 1)^2 + 3] .$$

Conclude that Fermat's claim about $p = x^2 + 3y^2$ holds.

Q11) Find (with proof!) a condition on when a positive integer N can be written in the form $N = x^2 + 3y^2$, $x, y \in \mathbb{Z}$.