Primes - Problem Sheet 2 - Solutions

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

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

Solution: A nice 'trick' to find these identities comes from factoring over $\mathbb{C}$. We have

$$x^2+y^2 = (x+iy)(x-iy) = (x+iy)\overline{(x+iy)}\,.$$

So

$$\begin{aligned}(x^2+y^2)(w^2+z^2) &= (x+iy)(w+iz)\overline{(x+iy)(w+iz)}\\ &= ((xw-yz)+i(xz+yw))\overline{((xw-yz)+i(xz+yw)}\\ &= (xw-yz)^2+(xz+yw)^2\end{aligned}$$

(The other sign comes from grouping $(x+iy)(w-iz)$ instead.)

So we obtain

$$(x^2+ny^2)(w^2+nz^2) = (xw \pm nyz)^2 + n(xz \mp yw)^2\,.$$

Then we can write

$$ax^2+cy^2 = a(x^2+\frac{c}{a}y^2)\,,$$

and use the above to get

$$(ax^2+cy^2)(az^2+cw^2) = (axw \pm cyz)^2 + ac(xz \mp yw)^2$$

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 $n=3$.

Solution: The 'obvious' candidate generalisation should be: Suppose $N = a^2+nb^2$, $\gcd(a,b)=1$. If $q = x^2+ny^2$, $\gcd(x,y)$ is a prime divisor of N, then $N/q = c^2+nd^2$, for some $\gcd(c,d)=1$.

The proof starts in the same way as for Lemma 2.5. We see that

$$q \mid x^2N - a^2q = n(xb-ay)(xb+ay)\,.$$

If $q \mid xb - ay$ or $q \mid xb + ay$, then without loss of generality, we can change $a \leftrightarrow -a$. So assume $q \mid xb - ay$, and continue as before. But it might be that $q \mid n$, for example $5 \mid 30 = 5^2 + 5 \times 1^2$. In this case, we obtain

$$q = x^2 + ny^2 \mid n\,,$$

so write $n = \alpha q$, with $\alpha \geq 1$. There is no solution with $y = 0$, so $y \geq 1$, and

$$q = x^2 + ny^2 \geq ny^2 \geq n \geq \alpha q\,.$$

Thus all $\geq$ are $=$, meaning $\alpha = 1$, and $q = n$.

Now if we have $N = a^2 + nb^2 = a^2 + qb^2$, then $q \mid N$ implies $q \mid a^2$ implies $q \mid a$. So

$$N/q = b^2 + q(a/q)^2$$

where $a/q \in \mathbb{Z}$.

If we take $q = 4$ (not prime!), and $n = 3$, we get to $4 \mid 3(xb - ay)(xb + ay)$. But since $4 = x^2 + 3y^2$, $\gcd(x, y)$ implies $x = y = 1$, we get $4 \mid 3(b - a)(b + a)$. The key step is to show that $4 \mid b - a$ or $4 \mid b + a$. But this must happen, else $2 \mid b - a$ and $4 \nmid b - a$ and $2 \mid b + a$ and $4 \nmid b + a$. So $a - b = 2k$, $a + b = 2l$, with k, l odd. Then $a = k + l$, $b = k - l$ which gives $\gcd(a, b) \geq 2$.

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?
Solution: It is not true: $p = 2$ divides $6 = 1^2 + 5 \times 1^2$, yet $2 \neq x^2 + 5y^2$. So the descent step fails 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 $p \equiv 1, 3 \pmod 8$.
Solution: The squares modulo 8 are $0^2, (\pm1)^2, (\pm2)^2, (\pm3)^2, (\pm4)^2 \equiv 0, 1, 4 \pmod 8$. So

$p = x^2 + 2y^2 \pmod 8$	$x = 0$	1	4
$y = 0$	0	1	4
1	2	3	6
4	0	1	4

So $p \equiv 0, 1, 2, 3, 4, 6 \pmod 8$. The only prime which can be $2, 4, 6 \pmod 8$ is $p = 2$. So we get

$$p = 2 \text{ or } p \equiv 1, 3 \pmod 8\,.$$

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.
Solution:

Setup: Suppose that $p \mid a^2 + 2b^2$ is an odd prime dividing $N = a^2 + 2b^2$, $\gcd(a, b) = 1$. We can assume $|a|, |b| < \frac{1}{2}p$ by changing $a \to a' = a + pk$ and $b \to b' = b + p\ell$. Then divide by $d = \gcd(a', b') > 1$. Certainly $p \nmid d^2$, otherwise $p \mid |a|, |b| < \frac{1}{2}p$ giving $a = b = 0$.

This means we can assume $p \mid N = a^2 + 2b^2$ with $\gcd(a, b) = 1$ and $N \leq \frac{1}{4}p^2 + \frac{2}{4}p^2 = \frac{3}{4}p^2$.

Any prime divisor $q \neq p$ of N is $< p$. Otherwise it is $> p$, and $N > pq > p^2$, contradicting the bound. Also $p^2 \nmid N$, so p only appears with exponent 1.

Descent: Suppose all such $q_i \mid N$ can be written as $x_i^2 + 2y_i^2$. Repeatedly apply Q2) to write $p = N/\prod q_i^{n_i}$ as $x^2 + 2y^2$.

So if p is not $x^2 + 2y^2$, then we can produce a smaller counter example $q < p$. This leads to an infinite decreasing sequence of prime numbers, which is a contradiction. Thus $p = x^2 + 2y^2$.

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:

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

Solution: If $p = 8k + 1$, then $(\mathbb{Z}/p\mathbb{Z})^*$ has order $8k$, and so every element $\beta \in (\mathbb{Z}/p\mathbb{Z})^*$ solves the above equation. The first factor can only have $4k$ solutions, so the second factor must have a solution. Let β be a solution to

$$(x^{2k} - 1)^2 + 2x^{2k}$$

Choose $b \equiv b \pmod p$, with $b > 0$. Then $p \mid (b^{2k} - 1)^2 + 2(b^k)^2$. We also have that $\gcd(b^{2k} - 1, b^k) = \gcd(-1, b^k) = 1$.

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

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

Solution:

Setup: Suppose p is an odd prime dividing $N = a^2 - 2b^2$. We can assume $|a|, |b| \leq \frac{1}{2}p$. Dividing by $\gcd(a, b)$ means we can assume

$$p \nmid N = a^2 - 2b^2$$

where $|N| \leq \frac{1}{4}p^2 + \frac{2}{4}p^2 = \frac{3}{4}p^2$.

Any prime divisor $q \neq p$ of $|N|$ is $< p$. Otherwise it is $> p$, and then $|N| \geq pq > p^2$, contradicting the bound. Similarly $p^2 \nmid N$, so p appears with exponent 1.

Descent: Suppose that all $q_i \mid N$ can be written as $x_i^2 - 2y_i^2$. One can check that the proof of item Q2) goes through since $n = 2$ is prime. So repeatedly apply this to write $p = N/\prod q_i^{n_i}$ as $x^2 - 2y^2$.

So if p is not $x^2 - 2y^2$, we can produce a smaller counter example $q < p$. This leads to an infinite decreasing sequence of primes numbers, which is a contradiction. Thus $p = x^2 - 2y^2$.

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

Solution: Assuming descent works for $x^2 - 2y^2$, and that $p \mid N = x^2-2y^2$, we conclude that $p = x^2-2y^2$. But reducing modulo 8 shows that $p = x^2 - 2y^2$ implies $p \equiv 1, 7 \pmod 8$. This contradicts the assumption that $p \equiv 3 \pmod 8$. If $2 \equiv a^2 \pmod p$, then we can write $p \mid a^2 - 2 \times 1^2$, which we have just shown is not possible. Hence $2 \not\equiv \Box \pmod p$.

c) Show p does not divide any $N = x^2 + y^2$.
Solution: From Fermat, we know $p \mid x^2 + y^2$ implies $p = x^2 + y^2$ implies $p \equiv 1 \pmod 4$. So $p \equiv 1, 5 \pmod 8$. But we assumed $p \equiv 3 \pmod 8$.

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.
Solution: If $a^2 \equiv b^2 \pmod p$, $a \neq b$, then $a \equiv \pm b \pmod p$. But $a \equiv -b \pmod p$ implies $a + b \equiv 0 \pmod p$ which is not possible since $1 \leq a, b \leq m$. On the other hand if $a \equiv b$, then we get $a = b$, since $1 \leq a, b \leq m$ and $p = 2m + 1$. So a, b are not distinct. Same words for $-a^2$ and $-b^2$.
Now if $a^2 \equiv -b^2$, then we get $p \mid a^2 + b^2$. Write $d = \gcd(a, b)$, then $p \mid d^2(a_0^2 + b_0^2)$. We can't have $p \mid d$, as $p \nmid a$. So $p \mid a_0^2 + b_0^2$, with $\gcd(a_0, b_0) = 1$. We showed above this is impossible.
So the set $\pm1^2, \pm2^2, \ldots, \pm m^2$ is exactly $1, 2, \ldots, 2m$, all non-zero residues modulo p. So $\pm a$ matches with $\pm n^2$, some n. If $a \neq n^2$, then $-a = n^2$. So one of $\pm a$ is a square.
From earlier we know 2 is no a square modulo p. Hence -2 must be a square modulo p.

e) Show that $p \mid x^2 + 2y^2$, with some $\gcd(x, y) = 1$. (Take $x = 1$.)
Solution: Write $-2 = a^2 \pmod p$, then $p \mid a^2 + 2 \cdot 1^2$.

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 $N = x^2 + 2y^2$, $x, y \in \mathbb{Z}$.
Solution: The proof is essentially the same as for $N = x^2 + y^2$. We obtain

$$N = x^2 + 2y^2$$

if and only if the primes $\equiv 5, 7 \pmod 8$ dividing N appear with even exponent.

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 $p \equiv 1 \pmod 3$.

Solution: The squares modulo 3 are $0^2, (\pm 1)^2 = 0, 1 \pmod 3$. So $p \equiv x^2 = 0, 1 \pmod 3$. The only prime which can be $\equiv 0 \pmod 3$ is 3. So $p = 3$ 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.
Solution:

Setup: Suppose p is an odd prime dividing $N = a^2 + 3b^2$. Can assume $|a|, |b| < \frac{1}{2}p$, so $N < \frac{1}{4}p^2 + \frac{3}{4}p^2 = p^2$.

Any prime divisor $q \neq p$ of N is $< p$, else $N > pq \geq p^2$, contradicting the bound. Also $p^2 \nmid p$, since $N < p^2$.

Descent: Notice that $2 \mid 1^2 + 3 \times 1^2$, but $2 \neq x^2 + 3y^2$, so the descent step fails here. So if descent fails for p, we must produce an odd prime $q < p$ for which is also fails.

I claim that if $2 \mid a^2 + 3b^2$, $\gcd(a, b) = 1$ then actually $4 \mid a^2 + 3b^2$. We have $a^2 + b^2 = (a + b)^2 = 0 \pmod 2$. So $a \equiv b \pmod 2$. Now, a, b cannot both be even, so they must both be odd. Reduce modulo 4, and we see $a^2 + 3b^2 \equiv a^2 - b^2 = 1^2 - 1^2 = 0 \pmod 4$. So in $a^2 + 3b^2$, 2 must appear to even power: we can repeatedly divide out 4 using **??**. This only stops when the result is odd.

Suppose that all odd primes $q_i < p$ are of the form $x_i^2 + 3y_i^2$. Then by repeatedly applying item Q2), including the case $q = 4$, we can write

$$p = N/(4^a \prod q_i^{n_i})$$

as $x^2 + 3y^2$. So if $p \neq x^2 + 3y^2$, one of the primes odd primes $q_i < p$ is a smaller counter example. This leads to an infinite decreasing sequence of odd primes, a contradiction. Hence $p = x^2 + 3y^2$.

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:

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

Solution: For $p = 3k + 1$, then $(\mathbb{Z}/p\mathbb{Z})^*$ has order $3k$, so every element $\beta \in (\mathbb{Z}/p\mathbb{Z})^*$ is a solution to the equation. (Notice that $p \nmid 4$, so $4 \not\equiv 0 \pmod p$). The first factor has k solutions, so the second factor must have $2k$ solutions. Let β be a solution. Then

$$p \mid (2\beta^k + 1)^2 + 3 \cdot 1^2$$

and we have $\gcd(2\beta^k + 1, 1) = 1$.

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 $N = x^2 + 3y^2$, $x, y \in \mathbb{Z}$.
Solution: The proof is essentially the same as for $N = x^2 + y^2$. We obtain

$$N = x^2 + 3y^2$$

if and only if the primes $p \equiv 2 \pmod 3$ (including $p = 2$) dividing N appear with even exponent.