Primes - Problem Sheet 1 - Solutions

Open ended questions for personal exploration

Try to get a feeling for some of the results discussed in the introduction lecture, by looking at the following questions. During the course, we will learn how to properly solve them. At the moment, no particular answers are expected!

Q1) 'Nice' congruence criteria exist for the following cases:

- $x^2 + 7y^2$ where discriminant $D = -28$,
- $x^2 - 5y^2$ where $D = 20$,
- $x^2 - 13y^2$ where $D = 52$,
- $x^2 + xy + 5y^2$ where $D = -19$,
- $x^2 + xy - y^2$ where $D = 5$,
- $x^2 + xy - 4y^2$ where $D = 17$.

Try to discover these conditions in one or two of the cases: which primes p can be written in these forms? What patterns do these p satisfy?

Perhaps you can write a computer program to investigate, or use a computer algebra system like Mathematica, Maple or Sage? Or even just a spreadsheet?

Solution: You might have noticed the introductory examples always have the congruence being either modulo D or $\frac{1}{4}D$. Either way, with some experimentation can find the following:

- x^2+7y^2 represents the following primes: $p = 7, 11, 23, 29, 37, 43, 53, 67, 71, 79, \ldots$. Except for $p = 2, 7$ these are exactly primes $p \equiv 1, 2, 4 \pmod 7$. (Also p square mod 7.)
- x^2-5y^2 represents the following primes: $p = 5, 11, 19, 29, 31, 41, 59, 61, 71, 79, 89, \ldots$. Except for $p = 5$, these are exactly primes $p \equiv 1, 4 \pmod 5$. (Also p square mod 5.)
- x^2-13y^2 represents the following primes: $p = 3, 13, 17, 23, 29, 43, 53, 61, 79, \ldots$. Except for $p = 13$, these are exactly primes $p \equiv 1, 2, 4, 9, 10, 12 \pmod{13}$. (Also p square mod 13.)
- $x^2+xy-5y^2$ represents the following primes: $p = 5, 7, 11, 17, 19, 23, 43, 47, 61, 73, 83, \ldots$. Except for $p = 19$, these are exactly primes $p \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \pmod{19}$. (Also p square mod 19.)
- x^2+xy-y^2 represents the following primes: $p = 5, 11, 19, 29, 31, 41, 59, 61, 71, 79, 89, \ldots$. Except for $p = 5$, these are exactlyprimes $p \equiv 1, 4 \pmod 5$. (Also p square mod 5.)
- $x^2+xy-4y^2$ represents the following primes: $p = 2, 13, 17, 19, 43, 47, 53, 59, 67, 83, 89, \ldots$. Except for $p = 2, 17$, these are exactly primes $p \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}$. (Also p square mod 17.)

Notice that with the $4 \mid D$ discriminants, $\frac{1}{4}D$ suffices in these examples. But generally, this doesn't hold. For example $x^2 - 3y^2$ represents primes

$p = 13, 37, 61, 73, 97, \ldots$. These are a strict subset of primes $p \equiv 1 \pmod 3$. However, they are exactly primes $p \equiv 1 \pmod{12}$. This is partly because $x^2 - 3y^2$ and $-x^2 + 3y^2$ are two non-equivalent quadratic forms of discriminant 12, and $-x^2 + 3y^2$ represents the remaining $p \equiv 7 \pmod{12}$ primes.

Q2) Recall the identity

$$\begin{aligned}&(2x^2 + 2xy + 3y^2)(2z^2 + 2zw + 3w^2)\\ &= (2xz + xw + yz + 3yw)^2 + 5(xw - yz)^2 .\end{aligned}$$

Try to find a similar identity for

$$(3x^2 + 2xy + 5y^2)(3z^2 + 2zw + 5w^2) = (\cdots)^2 + 14(\cdots)^2 \, ?$$

Solution: We want an identity which looks like

$$(3x^2+2xy+5y^2)(3z^2+2zw+5w^2) = (axz+bxw+cyz+dyw)^2+14(pxz+qxw+ryz+syw)^2$$

for some integers a, b, c, d, and p, q, r, s. Expanding out leads to a system of equations including

$$\begin{aligned}x^2z^2 : a^2 + 14p^2 = 9 &\rightsquigarrow a = \pm 3, p = 0\\ x^2w^2 : b^2 + 14q^2 = 15 &\rightsquigarrow b = \pm 1, q = \pm 1\\ y^2z^2 : c^2 + 14r^2 = 15 &\rightsquigarrow c = \pm 1, r = \pm 1\\ y^2w^2 : d^2 + 14s^2 = 25 &\rightsquigarrow d = \pm 5, s = 0\end{aligned}$$

We can fix $a = 3$, and $q = 1$, without loss of generality. Then testing the other coefficients leads to

$$(3x^2 + 2xy + 5y^2)(3z^2 + 2zw + 5w^2) = 14(wx - yz)^2 + (wx + 5wy + 3xz + yz)^2$$

Q3) Test the following criteria for various primes p to check they do work.

- Let p be a prime, then

$$p = x^2 + 27y^2 \text{ if and only if } \begin{cases} p \equiv 1 \pmod 3 \text{ , and} \\ 2 \equiv z^3 \pmod p \text{ has a solution} \end{cases}$$

- Let p be a prime, then

$$p = x^2 + 64y^2 \text{ if and only if } \begin{cases} p \equiv 1 \pmod 4 \text{ , and} \\ 2 \equiv z^4 \pmod p \text{ has a solution} \end{cases} .$$

- Let $p \neq, 2, 7$ be a prime, then

$$p = x^2 + 14y^2 \text{ if and only if } \begin{cases} -14 \equiv z^2 \pmod p \text{ has a solution, and} \\ (z^2+1)^2 \equiv 8 \pmod p \text{ has a solution} \end{cases} .$$

A good selection is $p = 23, 31, 43, 73, 89, 109, 113, 127, 137, 151, 157$. A computer algebra system like Maple, Mathematica or Sage might be helpful. Or perhaps just a spreadsheet.

Solution: We indicate a few examples in each case.

- By brute force, we see that $x^2 + 27y^2 = 73$ has no soution. (We need $y = 0, 1$, but this leads to $x = \sqrt{73}, \sqrt{46}$. We test that $73 = 3 \times 24 + 1 \equiv 1 \pmod 3$. But 2 is not a cube modulo 73, again a tedious brute force check.

On the other hand $109 = 1^2 + 27 \times 2^2$. And indeed $109 \equiv 3 \times 36 + 1 \equiv 1 \pmod 3$. Also $2 = 57^3 \pmod{109}$.

- We see that $3^2 + 14 \times 1^2 = 23$. Moreover $-14 = 3^2 \mod * 23$, and $8 = (3^2 + 1)^2 \pmod{23}$.
  On the other hand, $x^2 + 14y^2 = 157$ has no solution. We have $-14 = 65^2 \pmod{157}$. But $8 \not\equiv \square \pmod{157}$, so certainly $8 = (z^2+1)^2 \pmod{157}$ has no solution.