ELEMENTARY NUMBER THEORY

HOMEWORK 3

(1) Fermat repeatedly challenged English mathematicians by sending them problems he claimed to have solved and asking for proofs. Two of them were the following that he sent to Wallis:

- Prove that the only solution of $x^2+2=y^3$ in positive integers is given by $x=5$ and $y=3$;
- Prove that the only solution of $x^2+4=y^3$ in positive integers is given by $x=11$ and $y=5$.

In a letter to his English colleague Digby, Wallis called these problems trivial and useless, and mentioned a couple of problems that he claimed were of a similar nature:

- $x^2+12=y^4$ has unique solution $x=2$, $y=2$ in integers;
- $x^4+9=y^2$ has unique solution $x=2$, $y=5$ in integers;
- $x^3-y^3=20$ has no solution in integers;
- $x^3-y^3=19$ has unique solution $x=3$, $y=2$ in integers.

When Fermat learned about Wallis's comments, he called Wallis's problems mentioned above "amusements for a three-day arithmetician" in a letter to Digby. In fact, while Fermat's problems were hard (and maybe not even solvable using the mathematics known in his times), Wallis's claims are easy to prove. Do this.

Fermat's problems are difficult; in my opinion, he did not have proofs for these claims himself. Known solutions of these two problems involve algebraic number theory (we might come back to these in a few weeks). Also note that by integers I meant (of course) positive integers; in Fermat's days, negative numbers were not universally accepted.

- $x^2+12=y^4$ has unique solution $x=2$, $y=2$ in integers;
  Write $12=y^4-x^2=(y^2-x)(y^2+x)$. Since the two factors have the same parity, and since the product is even, we must have $y^2-x=2$ and $y^2+x=6$ (since $x>0$, the first factor must be the smaller one). This gives $x=2$ and $y=2$ as the only solution.
- $x^4+9=y^2$ has unique solution $x=2$, $y=5$ in integers;
  Here $9=(y-x^2)(y+x^2)$. If both factors are equal to 3, then $x=0$; thus $y-x^2=1$ and $y+x^2=9$, giving the solution $x=2$ and $y=5$.
- $x^3-y^3=20$ has no solution in integers;
  Here $20=(x-y)(x^2+xy+y^2)$. Clearly x and y have the same parity, hence $x-y$ is even. Thus we get $x-y\in\{2,10\}$, and none of these values leads to integral solutions.
- $x^3-y^3=19$ has unique solution $x=3$, $y=2$ in integers.
  Here $19=(x-y)(x^2+xy+y^2)$ implies $x-y=1$ and $x^2+xy+y^2=19$, hence $x=3$ and $y=2$.

(2) Show that there are infinitely many primes of the form $p \equiv \pm 1 \bmod 8$ by modifying Euclid's proof.

Let $p_1 = 7, \ldots, p_n$ be your list of primes of the form $p \equiv \pm 1 \bmod 8$, and consider the number $N = (p_1 \cdots p_n)^2 - 2$. Note that $N \equiv 7 \bmod 8$. Every prime divisor p of N satisfies $(p_1 \cdots p_n)^2 \equiv 2 \bmod p$, hence $(2/p) = 1$, and this shows that $p \equiv \pm 1 \bmod 8$. Moreover, no such prime p is on the list since $p_i \mid N + 2$, and now $p_i \mid N$ would imply $p_i = 2$.

Also observe that the proof actually shows that there are infinitely many primes of the form $p \equiv 7 \mod 8$, because N must have a prime divisor of this form.

(3) Use Gauss's Lemma to show that -2 is a quadratic residue of an odd prime p if $p \equiv 1, 3 \bmod 8$. Imitate the proof of Fermat's 2-squares-theorem to show that primes $p \equiv 1, 3 \bmod 8$ can be written in the form $p = c^2 + 2d^2$ for integers c, d.

Assume that $p = 4k + 1$, and consider the half system[1] $\{1, 2, \ldots, 2k\}$. Then

$$\begin{aligned} -2 \cdot 1 &\equiv -2 \\ -2 \cdot 2 &\equiv -4 \\ &\cdots \\ -2 \cdot k &\equiv -2k \\ -2 \cdot (k+1) &\equiv -2k - 2 \equiv 2k - 1 \\ &\cdots \\ -2 \cdot 2k &\equiv -4k \equiv 1 \end{aligned}$$

modulo p. Since there are exactly k sign changes, we have $(\frac{-2}{p}) = (-1)^k$, i.e., $(\frac{-2}{p}) = +1$ or -1 according as $p \equiv 1 \bmod 8$ or $p \equiv 5 \bmod 8$.

The case $p = 4k - 1$ is treated similarly.

Now we know that $(\frac{-2}{p}) = 1$ for primes $p \equiv 1, 3 \bmod 8$. Write $a^2 \equiv -2 \bmod p$. By Thue, there exist positive $x, y < \sqrt{p}$ with $ay \equiv x \bmod p$. Thus $x^2 \equiv a^2 y^2 \equiv -2y^2 \bmod p$, hence p divides $x^2 + 2y^2$ with $0 < x^2 + 2y^2 < 3p$. This implies $p = x^2 + 2y^2$ or $2p = x^2 + 2y^2$. In the last case, $x = 2X$ must be even, and then $p = y^2 + 2X^2$.

[1] It is also possible to compute $(\frac{-2}{p})$ from the supplementary laws; but when I ask you to apply Gauss's Lemma in an exam, you will have no choice.