Math 40520 Theory of Number
Homework 9

Due Wednesday 10/28

Do 4.

1. Suppose $p \equiv 3 \pmod 4$ is a prime. Show that for any rational numbers x and y, not both 0, $v_p(x^2+y^2)$ is even. [Hint: Reduce to the case where x, y are integers.]

2. Suppose x, y, z, t are rational numbers. Show that there exist rational number a, b, c, d such that

$$(x^2+y^2)(z^2+t^2) = a^2+b^2 \text{ and } \frac{x^2+y^2}{z^2+t^2} = c^2+d^2.$$

   [Hint: Use complex numbers.]

3. Suppose $a \in \mathbb{Q}$. Show that $x^2+y^2 = a$ has a rational solution if and only if every prime $\equiv 3 \pmod 4$ showing up in the factorization of a does so with an even exponent. [Hint: Use the previous exercises.]

4. Use Hasse's local-global theorem to show that $x^2+y^2+z^2 = 2028$ has an integral solution, and therefore infinitely many rational solutions. (Note that 3 appears to exponent 1 in 2028 so $x^2+y^2 = 2028$ has no rational solution, by the previous exercise.)

5. Parametrize all the rational solutions to $x^2+2y^2+3z^2 = 9$.

6. Find all primes p such that p^2+2 is also a prime.

7. Show that if p is a prime and $n = 2^p - 1$ then $2^n \equiv 2 \pmod n$. (This would be a consequence of Fermat's little theorem if n were a prime and the point of the exercise is to show this always, whether or not n is a prime.) [Hint: Use the fact that, since p is a prime, $2^p \equiv 2 \pmod p$.]

8. Show that if k is a positive integer and $n = 2^{2^k}+1$ then $2^n \equiv 2 \pmod n$. (This would be a consequence of Fermat's little theorem if n were a prime and the point of the exercise is to show this always, whether or not n is a prime.)