INTRODUCTION TO NUMBER THEORY PROBLEM SHEET 2

Solve the given problems and show ALL of your work, each answer should be justified by a sound mathematical argument. The ones tagged with $(*)$ should be submitted on Gradescope by 11:59 on October 12, following the link on the KEATs page.

Exercise 1. (1) Prove Lemma 2.4 from lectures:

Lemma 2.4. Let
$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$
with the p_i distinct primes and the a_i positive integers.

(a) $d > 0$ is a divisor of n if and only if
$$d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$
with $0 \leq b_i \leq a_i$ for each i.

(b) The number of positive divisors of n is $\prod_{i=1}^{r}(a_i + 1)$.

(2) How many positive common divisors do 100000 and 40000 have?

Exercise 2. Are the following statements true or false, where a and b are positive integers and p is prime? In each case, give a proof or counterexample:

(1) if $\gcd(a, p^2) = p$ then $\gcd(a^2, p^2) = p^2$
(2) if $\gcd(a, p^2) = p$ and $\gcd(b, p^2) = p^2$ then $\gcd(ab, p^4) = p^3$
(3) if $\gcd(a, p^2) = p$ and $\gcd(b, p^2) = p$ then $\gcd(ab, p^4) = p^2$
(4) if $\gcd(a, p^2) = p$ then $\gcd(a + p, p^2) = p$

Exercise 3. Write down a complete residue system modulo 17 composed entirely of multiples of 3.

Exercise 4 $(*)$. (1) Find all integer solutions of $x^3 + x^2 + x \equiv 0 \pmod{105}$.
(2) Find all integer solutions of $x^3 + x^2 + x + 1 \equiv 0 \pmod{143}$.
(3) Show that the equation $x^3 + x^2 - x + 3 = 0$ has no integer solutions.

Exercise 5 $(*)$. Show that there are infinitely many primes of the form $6k - 1$, with k a positive integer.

Exercise 6. (1) Suppose m is a positive integer and $2^m + 1$ is prime. Show that m is a power of 2. *Hint: if n is an odd positive integer then*
$$x^n + 1 = (x + 1)(x^{n-1} - x^{n-2} + \cdots + (-1)^i x^i + \cdots + 1)$$

As you can check, when $0 \leq n \leq 4$, $2^{2^n} + 1$ is prime. Fermat thought that $F_n = 2^{2^n} + 1$ might be prime for every $n \geq 0$...

(2) Use the equations $641 = 2^4 + 5^4 = 5 \times 2^7 + 1$ to show that
$$2^{32} \equiv -1 \pmod{641}$$
so F_5 is divisible by 641 and therefore isn't prime.

The only n for which F_n is known to be prime are $n = 0, 1, 2, 3, 4$.

Exercise 7. Suppose a and $m \geq 2$ are positive integers and $a^m - 1$ is prime. Show that $a = 2$ and m is prime.

Primes of the form $2^p - 1$ *with* p *prime are called Mersenne primes. The largest known primes are Mersenne primes (in January 2016, the largest known example was* $2^{74207281} - 1$*, since then two more examples have been found:* $2^{77232917} - 1$ *and* $2^{82589933} - 1$*), and for these large examples primality was established by a huge distributed computing project, the Great Internet Mersenne Prime Search.*