Lior Silberman's Math 312: Problem Set 5 (due 14/6/18)

Arithmetic functions

1. (A Mersenne prime)
   (a) Let p,q be primes such that $q|2^p-1$. Show that $q\equiv 1\,(p)$.
   Hint: Consider the order of 2 mod q.
   (b) Show that if p is odd then in fact $q\equiv 1\,(2p)$.
   Hint: $q-1$ is even.
   (*c) Prove that $n=2^{13}-1$ is prime by (i) Showing that if n were composite, it would be divisible by at least one of two specific primes and (ii) Explicitly dividing it with remainder by those primes to rule them out.

2. (a) Show that $f(n)=2^{\omega(n)}$ is a multiplicative function.
   Hint: Adapt the argument that proved that μ was multiplicative.
   (b) Show that $\sum_{d|n} f(d)=\tau(n^2)$.
   Hint: First show that it is enough to check when n is a prime power, then do that case.
   SUPP What would happen for $f(d)=b^{\omega(n)}$ for a general $b\in\mathbb{Z}_{\geq 2}$?

*3. Show that $\Lambda * I=\log$.
   Hint: The Use the prime factorization of the integer under consideration.

4. Define a function $\chi_4(n)=\begin{cases}1 & n\equiv 1\,(4)\\ -1 & n\equiv 3\,(4)\\ 0 & 2|n\end{cases}$ and set $s(n)=\sum_{d|n}\chi_4(d)$.
   (a) Show that χ_4 is completely multiplicative and conclude that s is multiplicative.
   (b) Calculate $s(2),s(3),s(4),s(5)$.
   (c) Let $r_2(n)=\#\left\{(a,b)\in\mathbb{Z}^2 \mid a^2+b^2=n\right\}$ be the number of ways to write n as a sum of two squares of integers (possibly negative!). Show that $r_2(n)=4s(n)$ for $n=2,3,4,5$.
   RMK The identity $r_2(n)=4s(n)$ holds for all n.

Cryptology

5. The following message has been encoded using an affine cipher. Decode it and explain your reasoning

```
NMCWT FIHHI ACPBN RSWHI NRUNG VSWBI BAUFS CPBAI YTHSI PNRSM
CTSCH HYIYW UMSFS NRSTG FGAGV SWCPB NRSYG YSFCN RWGEN AFCTS
```

   (Hint 1: the average frequency of letters in English falls according to ETAOIN)
   (Hint 2: the author of passage is the Rev. C.L. Dodgson, author of the book "Symbolic Logic Part I")

6. Show that in the following two affine ciphers encryption and decryption are the same operation (that is, that $E(E(P))=P$)
   (a) "ROT-13", a popular cipher for internet discussion boards, for which the encryption function is $E(P)\equiv P+13\,(26)$.
   (b) "Atbash", a historical cipher originally used in Hebrew, consisting of exchanging letters: $a\leftrightarrow z$, $b\leftrightarrow y$, $c\leftrightarrow x$ and so on. Its encryption function is $E(P)\equiv -1-P\,(26)$.

7. In this problem your will do an RSA decryption when the public key is $(e=5, m=2881)$.
   (a) Calculate $\phi(m)$ and find the decryption exponent d.
   (b) If the ciphertext is 0504 1874 0347 0515 2088 2356 0736 0468, what was the plaintext? (decrypt each four-digit number separately).
   (c) Interpret each resulting four-digit number as a pair of letters. What was the message?

Supplementary problems (not for submission)

A. Fix a prime p.
   (a) Let $f(x)=\sum_{i=0}^{n} a_i x^i$ be a polynomial with integer coefficients. Use the identity of PS2 problem 8 to show that $x-y$ divides $f(x)-f(y)$ as polynomials.
   (b) Let $c_1 \in \mathbb{Z}$ be such that $f(c_1) \equiv 0\,(p)$. Plugging in c_1 for y show that for some polynomial $g(x)$ with integer coefficients we have a congruence of polynomials $f(x) \equiv (x-c_1)g(x)\,(p)$. Moreover, $\deg(g) \leq \deg(f)-1$.
   (c) Let $c_2 \in \mathbb{Z}$ also be such that $f(c_2) \equiv 0\,(p)$ and assume that $c_1 \not\equiv c_2\,(p)$. Show that $g(c_2) \equiv 0\,(p)$.
   (d) Show by induction on r that if $\left\{c_j\right\}_{j=1}^{r}$ are representatives of the distinct congruence classes mod p which solve the equation $f(x) \equiv 0\,(p)$ then there is a polynomial $g(x)$ of degree$\leq n-r$ such that $f(x) \equiv g(x)\prod_{j=1}^{r}(x-c_j)$.
   (e) Show that if f is not zero mod p then has at most n distinct roots mod p.

B. Let f be an arithmetical function.
   (a) Show that f is invertible (there is g such that $f * g = \delta$) iff $f(1) \neq 0$.
   (b) Let f be invertible. Show that it has a unique inverse and that $\left(f^{-1}\right)^{-1} = f$.
   (c) Let f be invertible and multiplicative. Show that f^{-1} is multiplicative.