MATH 124, PROBLEM SET 3 (SOLUTIONS)

For the problem set due September 26, 2014:

1.) Here is a proof that is both slick and revelatory: Consider the n fractions $\frac{1}{n}, \dots, \frac{n}{n}$. Reducing to lowest terms will leave the various divisors of n in the denominators. For each divisor d, exactly $\phi(d)$ of these reduced fractions will have d in the denominator. To see why, note that d of the n fractions are equivalent to $\frac{1}{d}, \dots, \frac{d}{d}$, exactly $\phi(d)$ of which will not further reduce and thus have a final denominator of d. This partitions the n numbers, giving $\sum_{d|n} \phi(d) = n$.

2.) Answers may vary:

a) The public key is composed of two parts: the modulus $n = pq = (47)(31) = 1457$, and a number e coprime to and less than $\phi(n) = (p-1)(q-1) = 1380$, e.g., 7.

b) Person B sends the value $m^e \pmod{n}$, which in this case is $11^7 \equiv 1253 \pmod{1457}$.

3.) Gauss' lemma states that in this case, $\left(\frac{2}{p}\right) = (-1)^{\mu}$, where μ is the number of $2, 2\cdot 2, \dots, ((p-1)/2)\cdot 2$ which are greater than $\frac{p-1}{2}$. Let m be determined by $2m \le (p-1)/2$ and $2(m+1) > (p-1)/2$. Then $\mu = (p-1)/2 - m$.

- $p = 8k+1$ gives $(p-1)/2 = 4k$ and $m = 2k$. Then $\mu = 2k$, so $\left(\frac{2}{p}\right) = +1$.
- $p = 8k+3$ gives $(p-1)/2 = 4k+1$ and $m = 2k$. Then $\mu = 2k+1$, so $\left(\frac{2}{p}\right) = -1$.
- $p = 8k+5$ gives $(p-1)/2 = 4k+2$ and $m = 2k+1$. Then $\mu = 2k+1$, so $\left(\frac{2}{p}\right) = -1$.
- $p = 8k+7$ gives $(p-1)/2 = 4k+3$ and $m = 2k+1$. Then $\mu = 2k+2$, so $\left(\frac{2}{p}\right) = +1$.

4.) Applying Question 3, the values of $\left(\frac{-1}{p}\right)$, and multiplicativity:

a) $\left(\frac{-23}{83}\right) = \left(\frac{60}{83}\right) = \left(\frac{2}{83}\right)\left(\frac{2}{83}\right)\left(\frac{3}{83}\right)\left(\frac{5}{83}\right) = \left(\frac{3}{83}\right)\left(\frac{5}{83}\right) = -\left(\frac{83}{3}\right)\left(\frac{83}{5}\right) = -\left(\frac{2}{3}\right)\left(\frac{3}{5}\right) = -(-1)(-1) = -1$.

b) $\left(\frac{119}{139}\right) = \left(\frac{7}{139}\right)\left(\frac{17}{139}\right) = -\left(\frac{139}{7}\right)\left(\frac{139}{17}\right) = -\left(\frac{6}{7}\right)\left(\frac{3}{17}\right) = -\left(\frac{-1}{7}\right)\left(\frac{17}{3}\right) = -(-1)\left(\frac{2}{3}\right) = -1$.

Remark. Proceeding with $\left(\frac{119}{139}\right) = -\left(\frac{139}{119}\right)$ is not valid since $119 = 7 \times 17$, i.e., not prime.

5.) Implicitly, our divisors in the summation notation are comprehended over $\mathbb{N}$.

a) Rephrasing the sum as the more "symmetric" expression

$$(f * g)(n) = \sum_{dd'=n} f(d)g(d')$$

makes commutativity obvious.

b) $(f * id)(n) = \sum_{d|n} f(d) id\left(\frac{n}{d}\right)$. The id factor is only non-zero when $\frac{n}{d} = 1$, i.e., $d = n$. Thus the sum collapses to $f(n)$ (since commutativity is established, we do not need to verify that it is a left identity).

c) By part (a), we have

$$\begin{aligned}(f * (g * h))(n) &= \sum_{aa'=n} f(a)(g*h)(a') = \sum_{aa'=n} f(a)\left(\sum_{bc=a'} g(b)h(c)\right) \\ &= \sum_{aa'=n}\sum_{bc=a'} f(a)g(b)h(c) = \sum_{abc=n} f(a)g(b)h(c).\end{aligned}$$

Similarly,

$$((f*g)*h)(n) = \sum_{c'c=n}(f*g)(c')h(c) = \sum_{c'c=n}\left(\sum_{ab=c'} f(a)g(b)\right)h(c)$$
$$= \sum_{c'c=n}\sum_{ab=c'} f(a)g(b)h(c) = \sum_{abc=n} f(a)g(b)h(c),$$

and thus $f*(g*h) = (f*g)*h$.

6.) Note that for square-free numbers n, the last two cases can be folded into $(-1)^k$ where k is the number of (distinct) prime factors of n.

a) Let $(m,n)=1$. If either is not square-free, then the product mn is not square-free and $\mu(mn) = \mu(m)\mu(n) = 0$. Otherwise they are both square-free. Let m have a distinct prime factors and n have b distinct prime factors. These sets of prime factors do not overlap. Then $\mu(m)\mu(n) = (-1)^a(-1)^b = (-1)^{a+b} = \mu(mn)$.

b) Note that $\sum_{d|n}\mu(d) = \mu(1) = 1$, since 1 has an even (i.e., zero) number of prime factors. Let $n>1$. Then we can write $n = p_1^{a_1}\cdots p_k^{a_k}$. The square-free divisors of n are of the form $p_1^{\epsilon_1}\cdots p_k^{\epsilon_k}$ where $\epsilon_i \in \{0,1\}$. Hence

$$\sum_{d|n}\mu(d) = \sum_{(\epsilon_1,\ldots,\epsilon_k)\in\{0,1\}^k}\mu(p_1^{\epsilon_1}\cdots p_k^{\epsilon_k}).$$

Each summand is equal to $(-1)^m$, where m is the number of non-zero ϵ_i. Decompose the sum into the number of ways that no ϵ_i is non-zero, that one ϵ_i is non-zero, etc. Therefore our sum is equal to

$$\binom{k}{0} - \binom{k}{1} + \binom{k}{2} - \cdots + (-1)^k = (1-1)^k = 0,$$

following from the binomial theorem.

c) $\mu * F = \mu*(f*I) = \mu*f*I = f*(\mu*I) = f*id = f$.

d) Let x denote the function such that $x(n)=n$. In Question 1, we proved that $\phi*I = x$. Hence $x*\mu = (\phi*I)*\mu = \phi*(I*\mu) = \phi*id = \phi$.

Remark. It's amazing how observing underlying algebraic structure makes the reasoning behind otherwise messy symbol-pushing transparent.