COT4115.001S15 - HOMEWORK 00 (ANSWERS)
DUE JANUARY 15, 2015

Show all work (including any computer code) for full credit.

Question 1 (20 pts)**.**

(1) Explain the difference between message secrecy and message integrity? How are they related? Justify your answer.

Answer: Message secrecy concerns keeping a message concealed from unauthorized parties, while message integrity deals with preserving the message from noise or outside interference. In many cryptographic systems, any change to the ciphertext will make the message undecryptable.

(2) Give an example of where a symmetric key system would be preferable to a public key system, and vice versa. Justify your answer.

Answer: Many possible answers; in general, a public key is perferable in a context where anyone can encrypt but a limited few (or one) can decrypt, such as a connection to a secure web sever. A symmetric key system is preferable when both encryption and decryption are limited to a few parties, like when spies pass "top secret" messages to each other.

Question 2 (20 pts)**.**

(1) Compute:

$$\gcd\left(2^5 \cdot 3^3 \cdot 5^6 \cdot 11^2,\ 2^4 \cdot 3^3 \cdot 7^2 \cdot 11^1\right).$$

Answer: Find the largest prime powers that both numbers have in common:

$$2^4 \cdot 3^3 \cdot 11^1 = 4,752$$

(2) Using the Euclidean Algorithm, compute:

$$\gcd\left(161733,\ 234175\right).$$

Answer: $\gcd(\,161733,\,234175\,) = 29$

$$\begin{aligned}
234,175 &= 1 \cdot 161,733 + 72,442 \\
161,733 &= 2 \cdot 72,442 + 16,849 \\
72,442 &= 4 \cdot 16,849 + 5,046 \\
16,849 &= 3 \cdot 5,046 + 1,711 \\
5,046 &= 2 \cdot 1,711 + 1624 \\
1,711 &= 1 \cdot 1,624 + 87 \\
1,624 &= 18 \cdot 87 + 58 \\
87 &= 1 \cdot 58 + 29 \\
58 &= 2 \cdot \mathbf{29} + 0
\end{aligned}$$

Question 3 (30 pts)**.** Let a, b, q_i, r_i be as in Section 3.1.

(1) Let d be a common divisor of a, b. Show that $d \mid r_1$, and use this to show that $d \mid r_2$.

Answer: We are given that $a = q_1 b + r_1$ for some $q_1, r_1 \in \mathbb{Z}$ where $0 \leq r < b$. Since d divides both a and b, there exist $k_1, k_2 \in \mathbb{Z}$ such that $a = k_1\ d$ and $b = k_2\ d$. This means that $d\ k_1 = a = q_1\ b + r_1 = q_1\ (k_2\ d) + r_1$ which, rearranged, gives $r_1 = (k_1 - k_2)\ d$. Likewise $r_2 = b - q_2\ r_1$ which, by substitution, can be expressed as:

$$r_2 = (k_2\ d) - q_2\ (k_1 - k_2)\ d = (2\ k_2 - q_2\ k_1)\, d.$$

(2) Let d be as in (1). Use induction to show that $d \mid r_i$ for all i. In particular, $d \mid r_k$, the last nonzero remainder.

Answer: From part (1), $d \mid r_1, r_2$, so the initial cases of the induction are true. Assume that $d \mid r_i$ for each $r_1, r_2, \ldots, r_j$, and consider that $r_{j+1} = r_{j-1} - q_{r+1} r_j$. By the inductive hypothesis, $d \mid r_{j-1}$ and $d \mid r_j$, so $d \mid (r_{j-1} + q_{r+1} r_j) = r_{j+1}$.

(3) Use induction to show that $r_k \mid r_i$ for $1 \leq i \leq k$.

Answer: The last line of the Euclidean algorithm gives that $r_{k-1} = q_{k+1}\, r_k$, i.e., $r_k \mid r_{k-1}$ (this and the fact that $r_k \mid r_k$ provides the base cases for induction). Now suppose that $r_k \mid r_{j+1}$ and $r_k \mid r_j$, and consider $r_{j-1} = q_{j+1} r_j + r_{j+1}$. Since $r_k \mid r_{j+1}$ and $r_k \mid r_j$, it follows that

$$r_k \mid (q_{j+1} r_j + r_{j+1}) = r_{j-1}.$$

Thus, $r_k \mid r_i$ for $i = k, k-1, \ldots, 2, 1$.

(4) Using the facts that $r_k \mid r_1$ and $r_k \mid r_2$, show that $r_k \mid b$ and then $r_k \mid a$. Therefore, r_k is a common divisor of a, b.

Answer: From the context of Section 3.1, we have that $a = q_1 b + r_1$ and $b = q_2 r_1 + r_2$. From part (3), $r_k \mid r_2$ and $r_k \mid r_1$, so $r_k \mid (q_2 r_1 + r_2) = b$. Likewise $r_k \mid r_1$ and $r_k \mid b$, so $r_k \mid (q_1 b + r_1) = a$. Thus, r_k is a common divisor of both b and a.

(5) Use (2) to show that $r_k \geq d$ for all common divisors d, and therefore r_k is the greatest common divisor.

Answer: By part (2), we have that $d > 0$ and $d \mid r_k$ so $d \geq r_k$. However, d is the greatest common divisor of both a and b, so $r_k \leq d$. Therefore $r_k = d$.

Hint: This problem is in the solutions manual for the textbook (Chapter 3, **28.**). You may refer to their answer, but use your own words to receive credit.

Question 4 (30 pts)**.** Find the smallest integer $x \geq 50$ for which

$$\left| 1 - \frac{\pi(x)}{x/\log x} \right| < 0.06$$

where $\pi(x)$ is the prime-counting function.

Answer: This question relies on the ability to calculate $\pi(x)$ for large x. In Mathematica, this can be accomplished using the PrimePi[x] function. For example:

```
In[1]:  x = 50; While[ PrimePi[x] Log[x] / x > 1.06, x++ ]; x
Out[1]: 141,818,039
```