1 Exercises

1.1

Show that $a^6 \equiv 1 \pmod{14}$ for all a relatively prime to 14.

$$\begin{aligned}
1^6 &\equiv 1 \pmod{14} \\
3^6 &\equiv 1 \pmod{14} \\
5^6 &\equiv 1 \pmod{14} \\
9^6 \equiv (3^6)^2 &\equiv 1 \pmod{14} \\
11^6 &\equiv 1 \pmod{14} \\
13^6 &\equiv 1 \pmod{14}
\end{aligned}$$

1.2

Verify that Lemma 1 is true if $m = 14$ and $a = 5$.

$$\begin{gathered}
5 * 1 \equiv 5 \pmod{14} \\
5 * 3 \equiv 1 \pmod{14} \\
5 * 5 \equiv 11 \pmod{14} \\
5 * 9 \equiv 3 \pmod{14} \\
5 * 11 \equiv 13 \pmod{14} \\
5 * 13 \equiv 9 \pmod{14}
\end{gathered}$$

1.3

Verify that $3^{\phi(8)} \equiv 1 \pmod{8}$.

$\phi(8) = 4$, $3^4 \equiv (3^2)^2 \equiv 1 \pmod{8}$.

1.4

Which positive integers are less than 4 and relatively prime to it? What is the answer if 4 is replaced by 8? By 16? Can you induce a formula for $\phi(2^n), n = 1, 2, ...$?

4: 1, 3.
8: 1, 3, 5, 7.
16: 1, 3, 5, 7, 9, 11, 13, 15.
It will be all odd integers less than 2^n, since these are the only integers with no factor of 2 in their prime decomposition. So, $\phi(2^n) = 2^n/2 = 2^{n-1}$.

1.5

Verify that the formula is correct for $p = 5$ and $n = 2$.

Integers less than 25 that are relatively prime to 25:
1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24.
20 in all. $5^{2-1}(5-1) = 20$.

1.6

Calculate $\phi(74)$, $\phi(76)$, and $\phi(78)$.

$$\phi(74) = \phi(2)\phi(37) = 1 * 36 = 36$$
$$\phi(76) = \phi(2^2)\phi(19) = 2 * 18 = 36$$
$$\phi(78) = \phi(2)\phi(3)\phi(13) = 2 * 12 = 24$$

1.7

Calculate $\Sigma_{d|n}\phi(d)$
(a) For $n = 12, 13, 14, 15,$ and 16.
(b) For $n = 2^k, k \geq 1$.
(c) For $n = p^k, k \geq 1$ and p an odd prime.

(a) $\{d \ni d|12\} = \{1, 2, 3, 4, 6, 12\}$. $\Sigma_{d|n}\phi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$.
$\{d \ni d|13\} = \{1, 13\}$. $\Sigma_{d|n}\phi(13) = 1 + 12 = 13$.
$\{d \ni d|14\} = \{1, 2, 7, 14\}$. $\Sigma_{d|n}\phi(14) = 1 + 1 + 6 + 6 = 14$.
$\{d \ni d|15\} = \{1, 3, 5, 15\}$. $\Sigma_{d|n}\phi(15) = 1 + 2 + 4 + 8 = 15$.
$\{d \ni d|16\} = \{1, 2, 4, 8, 16\}$. $\Sigma_{d|n}\phi(16) = 1 + 1 + 2 + 4 + 8 = 16$.
(b) Know that $\{d \ni d|2^k\} = \{1, 2^1, ..., 2^k\}$. Also know that $\phi(2^k) = 2^{k-1}$, for $k \geq 1$.. So, $\Sigma_{d|n}\phi(2^k) = 1 + 2^0 + 2^1 + ... + 2^{k-1} = 1 + \frac{2^k-1}{2-1} = 2^k$.
(c) Know that $\{d \ni d|p^k\} = \{1, p^1, ..., p^k\}$. Also know that $\phi(p^k) = p^{k-1}(p-1)$. So, $\Sigma_{d|n}\phi(p^k) = 1 + p^0(p-1) + p^1(p-1) + ... + p^{k-1}(p-1) = 1 + (p-1)\frac{p^k-1}{p-1} = p^k$.

1.8

What are the classes C_d for $n = 14$?

$$C_1 = \{1, 3, 5, 9, 11, 13\}$$
$$C_2 = \{2, 4, 6, 8, 10, 12\}$$
$$C_7 = \{7\}$$
$$C_{14} = \{14\}$$

2 Problems

2.1

Calculate $\phi(42)$, $\phi(420)$, and $\phi(4200)$.

$$\phi(42) = \phi(2)\phi(3)\phi(7) = 1 * 2 * 6 = 12$$
$$\phi(420) = \phi(2^2)\phi(3)\phi(5)\phi(7) = 2 * 2 * 4 * 6 = 96$$
$$\phi(4200) = \phi(2^3)\phi(3)\phi(5^2)\phi(7) = 4 * 2 * 5 * 4 * 6 = 960$$

2.2

Calculate $\phi(54)$, $\phi(540)$, and $\phi(5400)$.

$$\phi(54) = \phi(2)\phi(3^3) = 1 * 3^2 * 2 = 18$$
$$\phi(540) = \phi(2^2)\phi(3^3)\phi(5) = 2 * 3^2 * 2 * 4 = 144$$
$$\phi(5400) = \phi(2^3)\phi(3^3)\phi(5^2) = 2^2 * 3^2 * 2 * 4 * 5 = 1440$$

2.3

Calculate ϕ of $10115 = 5 * 7 * 17^2$ and $100115 = 5 * 20023$.

$$\phi(10115) = \phi(5)\phi(7)\phi(17^2) = 4 * 6 * 17 * 16 = 6528$$
$$\phi(100115) = \phi(5)\phi(20023) = 4 * 20022 = 80088$$

2.4

Calculate ϕ of $10116 = 2^2 * 3^2 * 281$ and $100116 = 2^2 * 3^5 * 103$.

$$\phi(10116) = \phi(2^2)\phi(3^2)\phi(281) = 2 * 3 * 2 * 280 = 3360$$
$$\phi(100116) = \phi(2^2)\phi(3^5)\phi(103) = 2 * 3^4 * 2 * 102 = 33048$$

2.5

Calculate $a^8 \pmod{15}$ for $a = 1, 2, ..., 14$.

Since $\phi(15) = 8$, know by Euler's Theorem that $a^8 \equiv 1 \pmod{15}$ for all a for which $(a, 15) = 1$. That leaves us with $a \in \{3, 5, 6, 9, 10, 12\}$. Consider

$$\begin{aligned}
2 &\equiv 2 \pmod{15} \\
2^2 &\equiv 4 \pmod{15} \\
2^4 &\equiv 1 \pmod{15} \\
3 &\equiv 3 \pmod{15} \\
3^2 &\equiv 9 \pmod{15} \\
3^4 &\equiv 6 \pmod{15} \\
3^6 &\equiv 6 \pmod{15} \\
3^8 &\equiv 6 \pmod{15} \\
5 &\equiv 5 \pmod{15} \\
5^2 &\equiv 10 \pmod{15} \\
5^4 &\equiv 10 \pmod{15}
\end{aligned}$$

Can deduce from this that all the a that are by 3 and sometimes 2, i.e. $a \in \{3, 6, 9, 12\}$, are $\equiv 6 \pmod{15}$ when raised to the 8th power. The a that are divisible by 5 are $\equiv 10 \pmod{15}$ when raised to the 8th power.

2.6

Calculate $a^8 \pmod{16}$ for $a = 1, 2, ..., 15$.

Since $\phi(16) = 8$, know by Euler's Theorem that $a^8 \equiv 1 \pmod{16}$ for all the a for which $(a, 16) = 1$, i.e. all the odd a. All other a can be written $2k$, so $(2k)^8 = 2^4 2^4 k^8$ must be divisble by $16 = 2^4$, i.e. $a^8 \equiv 0 \pmod{16}$.

2.7

Show that if n is odd, then $\phi(4n) = 2\phi(n)$.

If n is odd, then it has no factor of 2 in its prime-power decomposition. Since ϕ is multiplicative, can then write $\phi(4n) = \phi(2^2)\phi(n) = 2\phi(n)$.

2.8

Perfect numbers satisfy $\sigma(n) = 2n$. Which n satisfy $\phi(n) = 2n$?

Write $n = p_1^{e_1}...p_k^{e_k}$ and $\phi(n) = n(1 - \frac{1}{p_1})...(1 - \frac{1}{p_k})$. Observe that since all $p_i > 1$, the product $(1 - \frac{1}{p_1})...(1 - \frac{1}{p_k})$ can't possibly be ≥ 1, let alone 2. This makes sense given the definition of ϕ as the number of positive integers less than or equal to n and relatively prime to n. Since there are only $n - 1$ integers less than or equal to n, the ceiling of $\phi(n)$ is $n - 1$.

2.9

$1+2 = (3/2)\phi(3), 1+3 = (4/2)\phi(4), 1+2+3+4 = (5/2)\phi(5), 1+5 = (6/2)\phi(6), 1+2+3+4+5+6 = (7/2)\phi(7)$, and $1+3+5+7 = (8/2)\phi(8)$. Guess a theorem.

$\Sigma_{d \ni (d,n)=1} = (n/2)\phi(n)$.

2.10

Show that

$$\Sigma_{p \leq x}\sigma(p) - \Sigma_{p \leq x}\phi(p) = \Sigma_{p \leq x}d(p)$$

Not sure if p is supposed to mean prime p, but I think so. If so, $\sigma(p_i) = 1 + p_i$, $\phi(p) = p_i - 1$, and $d(p_i) = 2$. So $\sigma(p_i) - \phi(p_i) = 2 = d(p_i)$. The relationship should hold for the sum as well.

2.11

Prove Lemma 3 by starting with the fact that there are integers r and s such that $ar + ms = 1$.

Lemma 3 states: if $(a, m) = 1$ and $a \equiv b \pmod{m}$, then $(b, m) = 1$. Per the prompt, multiply the congruence by r to get $ar \equiv br \pmod{m}$. We know that $ar \equiv ar + ms \equiv 1 \equiv br \pmod{m}$, or, in other words, that $m|br - 1$. Assume now that there is an integer d that divides m and b. Then $d|m$ and $d|br$. But if $d|m$, then $d|br - 1$, so it must be that $d|1$.

2.12

If $(a, m) = 1$, show that any x such that

$$x \equiv ca^{\phi(m)-1} \pmod{m}$$

satisfies $ax \equiv c \pmod{m}$.

Know that $a^{\phi(m)} \equiv 1 \pmod{m}$. Multiply both sides of the congruence to get $ax \equiv ca^{\phi(m)} \equiv c \pmod{m}$.

2.13

Let $f(n) = (n + \phi(n))/2$. Show that $f(f(n)) = \phi(n)$ if $n = 2^k$, $k = 2, 3, ...$

Know that $\phi(2^k) = 2^{k-1}$ So $f(2^k) = (2^k + 2^{k-1})/2 = 2^{k-2}3$. Observe that $\phi(3) = 2$, so $\phi(2^{k-2} * 3) = \phi(2^{k-2})\phi(3) = 2^{k-3} * 2 = 2^{k-2}$. So, $f(f(2^k)) = (2^{k-2}3 + 2^{k-2})/2 = 2^{k-2}2 = 2^{k-1} = \phi(2^k)$.

2.14

Find four solutions of $\phi(n) = 16$.

Can write $\phi(n) = p_1^{e_1-1}(p_1 - 1)...p_k^{e_k-1}(p_k - 1)$. Notice that $16 = 2^4$, so each term of this product must be a power of 2. So, possible $(p_i - 1)$ terms include be $p_i = 3, 5$. However, these p_i must have $e_i = 1$, otherwise we have $p_i^{e_i-1}$ terms which are not powers of 2. So, some possible n:

$$n = 2^5 = 32$$
$$n = 2^4 * 3 = 48$$
$$n = 2^3 * 5 = 60$$
$$n = 2^2 * 3 * 5 = 60$$

2.15

Find all solutions of $\phi(n) = 4$ and prove that there are no more.

Similarly to above, observe that $4 = 2^2$, and relevant primes from which to construct the number include 2, 3, and 5. We can exclude primes greater than 5 for the construction, since $5 - 1 = 2^2$, so for any $p_i > 5, p_i - 1 > 2^2$, which means its not a viable candidate. Likewise the n which include factors of 3 and 5 in their prime-power decompositions must have these at a factor of 1, for reasons outlined in the previous exercise. This leaves us with n of the form $2^{e_2}3^{e_3}5^{e_5}$, with $e_2 \in [0, 3]$ and $e_3, e_5 \in [0, 1]$. Can enumerate all such n that satisfy $\phi(n) = 4$: 5, 8, 10, 12.

2.16

Show that $\phi(mn) > \phi(m)\phi(n)$ if m and n have a common factor greater than 1.

If m, n have a common factor greater than 1, we know that they must share at least some of the primes of their prime-power decompositions, whose product we denote as $x = p_k^{\overline{e}_k} ... p_j^{\overline{e}_j}$. Now denote what remains of m and n's prime-power decompositions as $m/x = m'$, $n/x = n'$. Consider each p_i in the decomposition of x. It's possible that p_i divides either m' or n', but not both, since if it did, we would need to include an additional p_i term in x. So let's say that for each p_i, the p_i factor for one of either m' or n' is $\overline{e}_i$, and for the other it is $\overline{e}_i + \dot{e}_i$, where $\dot{e}_i \geq 0$. In mn we must thus have p_i with an exponent of $2\overline{e}_i + \dot{e}_i$. In $\phi(mn)$, we will have a term $p_i^{2\overline{e}_i + \dot{e}_i - 1}(p_i - 1)$ associated with p_i. In $\phi(m)\phi(n)$, the term associated with p_i is $p_i^{\overline{e}_i + \dot{e}_i - 1} p_i^{\overline{e}_i - 1}(p_i - 1)^2 = p_i^{2\overline{e}_i + \dot{e}_i - 2}(p_i - 1)^2$. The ratio of the p_i term in $\phi(mn)$ vs. $\phi(m)\phi(n)$ is $p_i/(p_i - 1) > 1$. The remaining primes in m' and n''s decompositions do not feature in x, and are unique between the two. So for each of these, the p_i term in $\phi(mn)$ is the same as that in $\phi(m)\phi(n)$.

2.17

Show that $(m, n) = 2$ implies $\phi(mn) = 2\phi(m)\phi(n)$.

Can write $m = 2 * p_1^{r_q} ... p_k^{r_k}$ and $n = 2^{e_2} * q_1^{s_1} ... q_k^{s_k}$ with all p_i different from all q_i (or reverse if m happens to have a higher power of 2 in its decomposition). For the p_i and q_i's, $\phi(2 * p_1^{r_q} ... p_k^{r_k} q_1^{s_1} ... q_k^{s_k}) = \phi(p_1^{r_q} ... p_k^{r_k})\phi(q_1^{s_1} ... q_k^{s_k})$ For the 2 factor, have an exponent of $e_2 + 1$ in mn, so in $\phi(mn)$ the term associated with 2 is $2^{e_2}(2 - 1) = 2^{e_2}$. In $\phi(m)\phi(n)$, the term associated with 2 is $2^0 * 1 * 2^{e_2 - 1} * 1 = 2^{e_2 - 1}$. So, $2\phi(m)\phi(n) = \phi(mn)$.

2.18

Show that $\phi(n) = n/2$ if and only if $n = 2^k$ for some positive integer k.

If $n = 2^k$, then $\phi(n) = 2^{k-1} = 2^k/2$. For the converse, observe that $\phi(n) = p_1^{e_1 - 1}(p_1 - 1) ... p_k^{e_k - 1}(p_k - 1) = p_1^{e_1} ... p_k^{e_k}/2$. Since $\phi(n) \in \mathbb{Z}$, $\phi(n) = n/2 \Rightarrow 2|n$, so know we have $p_1 = 2$. Furthermore, can write $n/2 = 2^{e_1 - 1} p_2^{e_2} ... p_k^{e_k} = 2^{e_1 - 1}(2 - 1) p_2^{e_2 - 1}(p_2 - 1) ... p_k^{e_k - 1}(p_k - 1)$. Dropping the $2^{e_1 - 1}$ term from both sides, need $p_2^{e_2 - 1}(p_2 - 1) ... p_k^{e_k - 1}(p_k - 1) = p_2^{e_2} ... p_k^{e_k}$ for this equation to hold. Note that $p_2^{e_2} ... p_k^{e_k}$ must be odd, since it explicitly excludes the factor associated with 2. But, $p_2^{e_2 - 1}(p_2 - 1) ... p_k^{e_k - 1}(p_k - 1)$ must be even, since it contains $p_i - 1$ terms. So, the only way for this to work if there are no factors than 2 in n, i.e. if $n = 2^k$.

2.19

Show that if $n - 1$ and $n + 1$ are both primes and $n > 4$, then $\phi(n) \leq n/3$.

Know that $2|n$, since both $n - 1$ and $n + 1$ odd. Also know that $3|n$, because if it did not, it would have to divide one of $n - 1$ or $n + 1$, and since $n - 1 \neq 3$ because $n > 4$, this would violate $n - 1$, $n + 1$ being prime. So can write $n = 2^{e_1} 3^{e_2} p_i^{e_i} ...$ and $\phi(n) = 2^{e_1 - 1} * 3^{e_2 - 1} * 2 * p_i^{e_i - 1}(p_i - 1) ... = 2^{e_1} * 3^{e_2 - 1} * p_i^{e_i - 1}(p_i - 1) ...$. So $3\phi(n) = 2^{e_1} * 3^{e_2} * p_i^{e_i - 1}(p_i - 1) ...$. If there are no prime factors p_i in n other than 2 and 3, then $3\phi(n) = n$. If there are, clearly each $p_i^{e_i - 1}(p_i - 1) < p_i * p_i^{e_i - 1} = p_i^{e_i}$, so $3\phi(n) < n$.

2.20

Show that $\phi(n) = 14$ is impossible.

Observe that the prime decomposition of 14 is $2 * 7$ and $\phi(n) = p_1^{e_1 - 1}(p_1 - 1)...p_k^{e_k - 1}(p_k - 1)$. None of the $(p_i - 1)$ terms can be 7, since 8 is not a prime. For the factor of 2, we could have $2^2|n$ or $3|n$. The term in $\phi(n)$ that would be associated with the term 2^2 in n is $2^1(2-1)$, which is clearly not divisible by 7. The term in $\phi(n)$ that would be associated with the term 3 in n is $3^0(3-1)$, which is also not divisible by 7. So, to get the term of 7 in $\phi(n)$, would need a term of 7^2 in n, but this is associated with a term of $7^1(7-1) > 14$.