1. Suppose that one domino can cover exactly two squares on a chessboard, either vertically or horizontally.

a. Can you tile an 8x8 chessboard with 32 dominos?

Yes. Tile each column vertically with 4 dominos.

6. Can you tile an 8x8 chessboard with 31 dominos if opposite corners are removed?

No.

c. Given a truncated chessboard, show how to construct a bipartite graph G that has a perfect matching if and only if the chessboard can be tiled with dominos.

Let the vertices be the spaces on the board.
The graph is 2-colorable/bipartite since a chessboard can be colored w/ 2 colors.
Divide the vertices into sets based on color (black/white)
Draw an edge between two vertices if a physical edge exists between those spaces.
If a perfect matching exists, then you can place a domino over each matched set of spaces, since each domino covers one black and one white space that share an edge, making the board tilable
If the board is tilable, then the perfect matching that exists is matching vertices that share a domino.

d. Based on this construction and Hall's theorem, can you state a necessary and sufficient condition for a truncated chessboard to be tilable with dominos? Try not to mention graphs or matching.

Condition: Every subset of white spaces in the truncated chessboard must have the same or a greater number of adjacent black spaces and visa versa.

Hall's theorem tells us: $\forall$ graph G whose vertices can be partitioned into two sets, L and R, $\ni$ every edge has one endpoint in L and one endpoint in R. There is a matching for the L vertices $\Leftrightarrow$ $|N(S)| \geq |S|$ for every $S \subseteq L$.

In c. we showed that G has a perfect matching $\Leftrightarrow$ the chessboard is tilable with dominos.

On our bipartite chess graph G, L = the set of white spaces and R = the set of black spaces.

Edges exist between spaces that share a physical edge (adjacent).

2. Prove that $\gcd(ka,kb) = k\gcd(a,b)\ \forall k>0$

Proof

Consider $k>0$

Consider $a,b \in \mathbb{Z}$

From theorem 3.1 in the notes, $\gcd(a,b) =$ the smallest linear combination of a and b.

So $\forall x,y \in \mathbb{Z}$ $x(a)+y(b) \geq \gcd(a,b)$ and $\exists\, c,d \in \mathbb{Z} \ni c(a)+d(b) = \gcd(a,b)$

So $\gcd(ka,kb) = c(ka)+d(kb) = k(c(a)+d(b))$ since $(c(a)+d(b))$ minimizes the sum.

Rewriting, this shows $\underline{\gcd(ka,kb) = k\gcd(ka,kb)}$ //

3. Suppose that $a \equiv b \pmod{n}$ and $n>0$. Prove or disprove the following assertions:

a. $a^c \equiv b^c \pmod{n}$ where $c \geq 0$

<u>Proof</u> by induction

<u>Induction hypothesis</u> $P(c)$: $a^c \equiv b^c \pmod{n}$ $c \in \mathbb{N} \cup \{0\}$

<u>Base cases</u>: $P(0)$: $a^0 = 1$ $b^0 = 1$

$1 \equiv 1 \pmod{n}$ since $a \equiv a \pmod{n}$

$P(1)$: $a \equiv b \pmod{n}$ from our problem statement

This forms a basis for induction.

<u>Inductive step</u>: $\forall n > 0 \in \mathbb{Z}$, for $c \geq 0$ $a^c \equiv b^c \pmod{n}$

Recall that $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow ac \equiv bd \pmod{n}$

Let $c = a^c$ and $b = a^c$

Then $aa^c = a^{c+1} \equiv bb^c = b^{c+1} \equiv \pmod{n}$

So $P(c) \Rightarrow P(c+1)$ for $\forall c > 0 \in \mathbb{Z}$

Thus by induction $P(c)$ holds for all $c > 0 \in \mathbb{Z}$

Thus $a \equiv b \pmod{n}$ $n > 0 \Rightarrow a^c \equiv b^c \pmod{n}$ where $c > 0$

b. $c^a \equiv c^b \pmod{n}$ where $a, b \geq 0$

This is false.

Let $a=4$, $b=1$, and $n=3$

Then $a \equiv b \pmod{n}$ since $3 \mid (4-1)$

$3 \mid 3$

Let $c=2$

In order for the assertion to hold the following must be true

$n \mid (c^a - c^b)$, however notice

$3 \mid (2^4 - 2)$

$\Rightarrow$ $3 \mid (8)$ which is clearly not true.

So $c^a \equiv c^b \pmod{n}$ is invalidated

4. An inverse of k modulo $n > 1$ is an integer, k^{-1}, such that

$$k \cdot k^{-1} \equiv 1 \pmod{n}$$

Show that k has an inverse iff $\gcd(k, n) = 1$.

<u>Proof</u>

Suppose $\gcd(k, n) = 1$

Therefore there exists a linear combination of n and k that equals 1

$\exists s, t \in \mathbb{Z} \ni sn + tk = 1$

Rewriting $sn = 1 - tk$

$\Rightarrow n \mid (1 - tk)$ by the definition of divisibility

$tk \equiv 1 \pmod{n}$ by the definition of congruence

Thus $\exists$ an inverse of k modulo n, namely t

Now suppose $\exists k^{-1} \in \mathbb{Z} \ni k \cdot k^{-1} \equiv 1 \pmod{n}$

Then $n \mid (1 - kk^{-1})$

$\Rightarrow \exists (s \in \mathbb{Z}) \ni sn = 1 - kk^{-1}$

Rewriting the above as $1 = sn + kk^{-1}$ shows there exists a linear combination of n and k that equals 1

Thus $\gcd(k, n) = 1$

So $\exists k^{-1} \in \mathbb{Z} \ni kk^{-1} \equiv 1 \pmod{n} \Leftrightarrow \gcd(k, n) = 1$ //

5. Here is a long run of composite numbers:
114, 115, ..., 126

Prove that there exist arbitrarily long runs of composite numbers.

Proof

Consider $n \in \mathbb{N}$

Consider $k \in \{\mathbb{N} \mid 1 < k \leq n\}$

$n! + k$ can be rewritten as $k\left(\prod_{i=1}^{k-1} i \prod_{j=k+1}^{n} j + 1\right)$

So $k \mid (n! + k) \Rightarrow n! + k$ is composite

Making $n!+2, n!+3, \ldots, n!+n$ a $n-1$ long run of composite numbers.

Since we chose n arbitrarily, we can construct an arbitrarily long run of composite numbers in the same way, confirming its existence //

6. Take a big number, such as 37273761261. Sum the digits, where every other digit is negated.

$$3+(-7)+2+(-7)+3+(-7)+6+(-1)+2+(-6)+1=-11$$

As it turns out, the original number is a multiple of 11 if and only if this sum is a multiple of 11.

a. Use this result from elsewhere on this problem set to show that:
$10^k \equiv -1^k \pmod{11}$

Notice $11 \mid (10-(-1))$
Then $10 \equiv -1 \pmod{11}$ from the definition of congruent
and $10^k \equiv -1^k \pmod{11}$ as shown in 3.a.

b. Using this fact, explain why the procedure above works.

Consider a large number n

We can write n in decimal form as

$n = \sum_{i=0}^{\lfloor \log_{10} n \rfloor} d_i 10^i$, where d_i is the ith digit.

Applying the result from part a we know $d_i 10^i \equiv d_i (-1)^i \pmod{11}$

So $n \equiv \sum_{i=0}^{\lfloor \log_{10} n \rfloor} d_i (-1)^i \pmod{11} \Rightarrow 11 \mid (n - (\text{alternating sum of the digits}))$

If k is even $d_k(-1)^k = d_k$, putting the alternating sum in the form of the problem statement. If k is odd, we can multiply the sums by -1 with no loss of generality because we are concerned only with divisibility.

If n is divisible by 11 and the alternating sum of digits is, then $n - (\text{alternating sum of the digits})$ also is, explaining why the procedure above works.

7. Let $S_k = \sum_{i=1}^{p-1} (i)^k$, where p is an odd prime and k is a positive multiple of $p-1$. Use Fermat's Theorem to prove that $S_k \equiv -1 \pmod p$

Proof

We know $x^{p-1} \equiv 1 \pmod p$ if x is not a multiple of p from Fermat's theorem.

So for $x \in \mathbb{Z}$, $1 \leq x < p$, $x^{p-1} \equiv 1 \pmod p$

$\exists\, a > 0 \in \mathbb{Z} \ni a(p-1) = k$ since k is a multiple of $p-1$

Then $x^k \equiv 1 \pmod p$ from 3.a.

Summing each side for $\forall (x < p) \in \mathbb{Z}^+$, $\sum_{i=1}^{p-1} (i)^k = (p-1) 1 \pmod p$

$\Rightarrow S_k \equiv -1 \pmod p$ since the p divides out. //