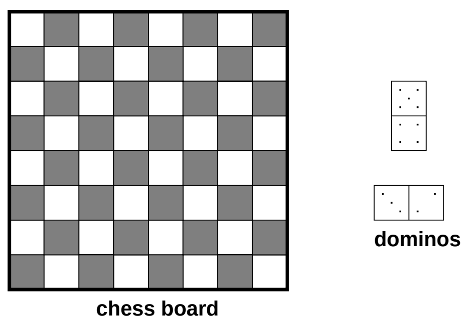
October 28
revised October 12, 2005, 909 minutes

Solutions to Problem Set 5

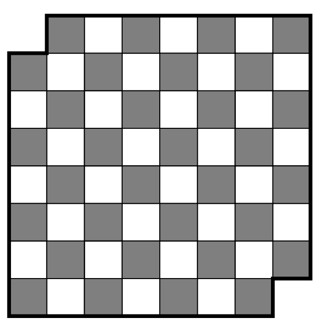
Problem 1. Suppose that one domino can cover exactly two squares on a chessboard, either vertically or horizontally.

(a) Can you tile an 8×8 chessboard with 32 dominos?



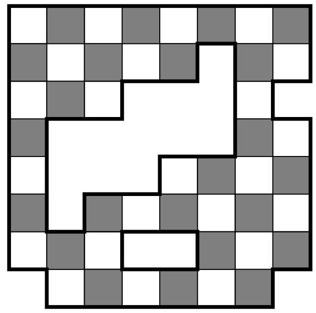
Solution. Yes. Place 4 vertical dominos in each column. ■

(b) Can you tile an 8×8 chessboard with 31 dominos if opposite corners are removed?



Solution. No! Opposing corners are the same color. Therefore, removing opposite corners leaves an unequal number of white and black squares. Since every domino covers one black square and one white square, no tiling is possible. ■

(c) Now suppose that an assortment of squares are removed from a chessboard. An example is shown below.



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.

Solution. Create a vertex for every white square and a vertex for every black square. Put an edge between squares that share an edge. (This graph is bipartite, since the coloring of the squares defines a valid 2-coloring of the vertices.)

If a perfect matching exists in this graph, then a tiling exists: put a domino over each pair of matched vertices. On the other hand, if a tiling exists, then a perfect matching exists: match squares covered by the same 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 matchings!

Solution. A board can be tiled with dominos if and only if every set of white squares is adjacent to at least as many black squares and vice versa. ■

Problem 2. Prove that $\gcd(ka, kb) = k \cdot \gcd(a, b)$ for all $k > 0$.

Solution. The smallest positive value of:

$$k \ \cdot \ (s \cdot a + t \cdot b)$$

(which is equal to $s(ka) + t(kb) = \gcd(ka, kb)$) must be k times the smallest positive value of:

$$s \cdot a + t \cdot b$$

(which is equal to $\gcd(a, b)$). ■

Problem 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 $c \geq 0$

Solution. The proof is by induction on c with the hypothesis that $a^c \equiv b^c \pmod{n}$. If $c = 0$, then the claim holds, because $1 \equiv 1 \pmod{n}$. Now suppose that:

$$a^c \equiv b^c \pmod{n}$$

Multiplying both sides by a gives:

$$a^{c+1} \equiv ab^c \pmod{n}$$

Since $a \equiv b \pmod{n}$, we can replaced the a on the right side by b:

$$a^{c+1} \equiv b^{c+1} \pmod{n}$$

Therefore, the claim holds by induction. ∎

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

Solution. The claim is false. For example:

$$2^0 \not\equiv 2^3 \pmod{3} \tag{1}$$

∎

Problem 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 $\gcd(k, n) = 1$. *Hint: We saw how to prove the above when n is prime.*

Solution. If $\gcd(k, n) = 1$, then there exist integers x and y such that $kx + yn = 1$. Therefore, $yn = 1 - kx$, which means $n \mid (1 - kx)$ and so $kx \equiv 1 \pmod{n}$. Let k^{-1} be x. ■

Problem 5. Here is a long run of composite numbers:

$$114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126$$

Prove that there exist arbitrarily long runs of composite numbers. Consider numbers a little bigger than $n!$ where $n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$.

Solution. Let k be some natural number such that $1 < k \leq n$. We know $k|(n! + k)$ because $k \mid n!$ and $k \mid k$. Thus, the numbers $n! + 2, n! + 3, n! + 4, \ldots, n! + n$ must all be composite. This is a run of $n - 1$ consecutive composite numbers. Because we can arbitrarily choose n, we know arbitrarily long runs of compisite numbers exist. ■

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

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

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

Solution. We know $10 \equiv -1 \pmod{11}$. From 2a, we conclude $10^k \equiv (-1)^k \pmod{11}$.

■

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

Solution. A number in decimal has the form:

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0$$

From the observation above, we know:

$$\begin{aligned} & d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0 \\ \equiv\ & d_k \cdot (-1)^k + d_{k-1} \cdot (-1)^{k-1} + \ldots \cdot + d_1 \cdot (-1)^1 + d_0 \cdot (-1)^0 \pmod{11} \\ \equiv\ & d_k - d_{k-1} + \ldots \cdot - d_1 + d_0 \pmod{11} \end{aligned}$$

Note that the above assumes k is even. The case where k is odd is analogous. Also, the procedure given in the problem may have us reverse all signs. Because we are only checking for divisibility, this does not matter. ■

Problem 7. Let $S_k = 1^k + 2^k + \ldots + (p-1)^k$, where p is an odd prime and k is a positive multiple of $p - 1$. Use Fermat's theorem to prove that $S_k \equiv -1 \pmod{p}$.

Solution. Fermat's theorem says that $x^{p-1} \equiv 1 \pmod{p}$ when $1 \leq x \leq p - 1$. Since k is a multiple of $p - 1$, raising each side to a suitable power proves that $x^k \equiv 1 \pmod{p}$. Thus:

$$\begin{aligned} 1^k + 2^k + \ldots + (p-1)^k &\equiv \underbrace{1 + 1 + \ldots + 1}_{p-1 \text{ terms}} \pmod{p} \\ &\equiv p - 1 \pmod{p} \\ &\equiv -1 \pmod{p} \end{aligned}$$

■