Solution *Section* 2.6 – Applications of Congurences

Exercise

Find the memory locations assigned by the hashing function $h(k) = k$ **mod** 97 to the records of customers with Social Security numbers?

a) 034567981 *b)* 183211232 *c)* 220195744 *d)* 987255335
e) 104578690 *f)* 432222187 *g)* 372201919 *h)* 501338753

Solution

a) $034567981 \ \textbf{mod}\ 97 = 91$

b) $183211232 \ \textbf{mod}\ 97 = 57$

c) $220195744 \ \textbf{mod}\ 97 = 21$

d) $987255335 \ \textbf{mod}\ 97 = 5$

e) $104578690 \ \textbf{mod}\ 97 = 80$

f) $432222187 \ \textbf{mod}\ 97 = 81$

g) $372201919 \ \textbf{mod}\ 97 = 18$

h) $501338753 \ \textbf{mod}\ 97 = 73$

Exercise

A parking lot has 31 visitor spaces, numbered from 0 to 30. Visitors are assigned parking spaces using the hashing function $h(k) = k$ **mod** 31, where k is the number formed from the first three digits on a visitor's license plate.

a) Which spaces are assigned by the hashing function to cars that have these first three digits on their license plates: 317, 918, 007, 100, 111, 310

b) Describe a procedure visitors should follow to find a free parking space, when the space they are assigned is occupied.

Solution

a) $317 \ \textbf{mod}\ 31 = 7$
$918 \ \textbf{mod}\ 31 = 19$
$007 \ \textbf{mod}\ 31 = 7$
$100 \ \textbf{mod}\ 31 = 7$
$111 \ \textbf{mod}\ 31 = 18$
$310 \ \textbf{mod}\ 31 = 0$

b) Take the next available space, where the next space is computed by adding 1 to the space number and pretending that 30 + 1 = 0.

Exercise

Find the sequence of pseudorandom numbers generated by the linear congruential generator

a) $x_{n+1} = \left(3x_n + 2\right)$ **mod** 13 with seed $x_0 = 1$.

b) $x_{n+1} = \left(4x_n + 1\right)$ **mod** 7 with seed $x_0 = 3$.

Solution

a) Given $x_0 = 1$, the $x_1 = \left(3x_0 + 2\right) \textbf{\textit{mod}}\ 13 = \left(3 \cdot 1 + 2\right) \textbf{\textit{mod}}\ 13 = 5 \textbf{\textit{ mod}}\ 13 = 5$

$x_2 = \left(3 \cdot 5 + 2\right) \textbf{\textit{mod}}\ 13 = 17 \textbf{\textit{ mod}}\ 13 = 4$

$x_3 = \left(3 \cdot 4 + 2\right) \textbf{\textit{mod}}\ 13 = 14 \textbf{\textit{ mod}}\ 13 = 1$

The sequence keep continue to repeat 1, 5, 4, 1, 5, 4, …

b) Given $x_0 = 3$, the $x_1 = \left(4x_0 + 1\right) \textbf{\textit{mod}}\ 7 = \left(4 \cdot 3 + 1\right) \textbf{\textit{mod}}\ 7 = 13 \textbf{\textit{ mod}}\ 7 = 6$

$x_2 = \left(4 \cdot 6 + 1\right) \textbf{\textit{mod}}\ 7 = 25 \textbf{\textit{ mod}}\ 7 = 4$

$x_3 = \left(4 \cdot 4 + 1\right) \textbf{\textit{mod}}\ 7 = 17 \textbf{\textit{ mod}}\ 7 = 3$

The sequence keep continue to repeat 3, 6, 4, 3, 6, 4, …

Exercise

Find the sequence of pseudorandom numbers generated by using the pure multiplicative generator $x_{n+1} = 3x_n$ **mod** 11 with seed $x_0 = 2$.

Solution

$x_1 = 3x_0$ **mod** $11 = 3 \cdot 2$ **mod** $11 = 6$

$x_2 = 3x_1$ **mod** $11 = 3 \cdot 6$ **mod** $11 = 18$ **mod** $11 = 7$

$x_3 = 3x_2$ **mod** $11 = 3 \cdot 7$ **mod** $11 = 21$ **mod** $11 = 10$

$x_4 = 3x_3$ **mod** $11 = 3 \cdot 10$ **mod** $11 = 30$ **mod** $11 = 8$

$x_5 = 3x_4$ **mod** $11 = 3 \cdot 8$ **mod** $11 = 24$ **mod** $11 = 2$

Since $x_5 = x_0$, the sequence repeats forever: 2, 6, 7, 10, 8, 2, 6, 7, 10, 8, …

Exercise

The first nine digits of the ISBN-10 of the European version of the fifth edition of this book are $0 - 07 - 119881$. What is the check digit for that book?

Solution

Let *d* be the check digit.

$1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 1 + 5 \cdot 1 + 6 \cdot 9 + 7 \cdot 8 + 8 \cdot 8 + 9 \cdot 1 + 10 \cdot d \equiv 0 \left(\textbf{\textit{mod}}\ 11\right)$

$213+10\cdot d\equiv 0(\textbf{mod } 11)$

So $213\equiv 4(\textbf{mod } 11)$ *and* $10\equiv -1(\textbf{mod } 11)$

This is equivalent to: $4-d\equiv 0(\textbf{mod } 11)$ or $\underline{d=4}$

Exercise

The ISBN-10 of the sixth edition of Elementary Number Theory and Its Applications is $0-321-500Q1-8$, where Q is a digit. Find the value of Q.

Solution

$1\cdot 0+2\cdot 3+3\cdot 2+4\cdot 1+5\cdot 5+6\cdot 0+7\cdot 0+8\cdot Q+9\cdot 1+10\cdot 8\equiv 0(\textbf{mod } 11)$

$130+8Q\equiv 0(\textbf{mod } 11)$

$8Q\equiv -130(\textbf{mod } 11)\equiv 2(\textbf{mod } 11)$ $\quad -130\equiv(-12\cdot 11+2)(\textbf{mod } 11)$

$8Q\equiv 2(\textbf{mod } 11)$ Since $24\equiv 2(\textbf{mod } 11)$

Therefore $8Q=24$

This is equivalent to: $\underline{Q=3}$

Exercise

The USPS sells money orders identified by 11-digit number $x_1, x_2, \ldots, x_{11}$. The first ten digits identify the money order: x_{11} is a check digit that satisfies $x_{11}=x_1+x_2+\cdots+x_{10}$ **mod** 9. Find the check digit for the USPS money orders that have identification number that start with these ten digits

a) 7555618873	*b)* 6966133421	*c)* 8018927435	*d)* 3289744134
e) 74051489623	*f)* 88382013445	*g)* 56152240784	*h)* 66606631178

Solution

a) $(7+5+5+5+6+1+8+8+7+3)\textbf{mod } 9=55\,\textbf{mod } 9=1$

b) $(6+9+6+6+1+3+3+4+2+1)\textbf{mod } 9=41\,\textbf{mod } 9=5$

c) $(8+0+1+8+9+2+7+4+3+5)\textbf{mod } 9=47\,\textbf{mod } 9=2$

d) $(3+2+8+9+7+4+4+1+3+4)\textbf{mod } 9=45\,\textbf{mod } 9=0$

e) $(7+4+0+5+1+4+8+9+6+2+3)\textbf{mod } 9=49\,\textbf{mod } 9=4$

f) $(8+8+3+8+2+0+1+3+4+4+5)\textbf{mod } 9=46\,\textbf{mod } 9=1$

g) $(5+6+1+5+2+2+4+0+7+8+4)\textbf{mod } 9=44\,\textbf{mod } 9=8$

h) $(6+6+6+0+6+6+3+1+1+7+8)\textbf{mod } 9=50\,\textbf{mod } 9=5$

Exercise

Determine which single digit errors are detected by the USPS money order code.

Solution

If one digit change to a value not congruent to it modulo 9, then the modular equivalence implied by the equation in the preamble will no longer hold. Therefore all single digit errors are detected except for the substitution of a 9 for a 0 or vice versa.

Exercise

Determine which transposition errors are detected by the USPS money order code.

Solution

Because the first ten digits are added, any transposition error involving them will go undetected. The sum of the first ten digits will be the same for the transposed number as it is for the correct number.

Suppose that the last digit is transposed with another digit; without loss of generality; we can assume it's the tenth digit and that $x_{10} \neq x_{11}$.

Then the correct equation will be

$$x_{11} \equiv x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} \pmod 9 \qquad (1)$$

But the equation resulting from the error will read

$$x_{10} \equiv x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{11} \pmod 9 \qquad (2)$$

Subtract equations (2) & (1)

$$x_{11} - x_{10} \equiv x_{10} - x_{11} \pmod 9$$

$$2x_{11} \equiv 2x_{10} \pmod 9 \qquad \textit{Divide by 2 both sides since 2 is prime}$$

$$x_{11} \equiv x_{10} \pmod 9 \quad \text{Which is false}$$

The check equation will fail.

Therefore we conclude that transposition errors involving the eleventh digits are detected.