1 Counting Soldiers

After a terrible battle against Mongols, general Li wants to count how many soldiers came back. He can see approximately 100 tired men. He asks them to form 7 columns inline. There are 7 soldiers on every line except the last one which has 3. Then he does the same with 11 columns and see that the last line only has 9 soldiers.

How many soldiers are there?

2 Pairwise Different Sampling

We throw an unbiased dice 12 times and get the samples $x_1, \ldots, x_{12} \in \{1, \ldots, 6\}$. We define pairs $y_1 = (x_1, x_2), \ldots, y_6 = (x_{11}, x_{12})$.

What is the probability that the $y_i$’s are pairwise different? Can you explain this result?

3 RSA Parameters

As a toy example we want to use RSA with modulus $N = 29 \times 31 = 899$. We want to compute $x^e \mod N$ using the square-and-multiply algorithm.

Give eligible values for $e$ and compute how many multiplications are needed in this algorithm. What is the best $e$?