Probabilistic proofs
A vertex colouring with $k$ colours of a graph $G = (V, E)$ is a mapping $\gamma : V \rightarrow \{1, \ldots, k\}$, such that $\gamma(u) \neq \gamma(v)$ for any edge $(u, v) \in E$.

The chromatic number $\chi(G)$ of a graph $G$ is the smallest $k$, such that $G$ has vertex colouring with $k$ colours.

The girth $g(G)$ of a graph $G$ is the length of the shortest cycle in $G$.

A graph with a large girth “locally looks” like a tree. Trees can be coloured with two colours. Nevertheless

Theorem. For any $k \in \mathbb{N}$ there exists a graph $G$, such that $g(G) > k$ and $\chi(G) > k$.

Proof follows...
A *probability distribution* on a set $X$ is a function $\mu : X \rightarrow [0, 1]$, such that $\sum_{x \in X} \mu(x) = 1$.

(we assume that $X$ is finite)

An *event* on a set $X$ is a subset $A \subseteq X$.

Let $\mu$ be fixed. Then $\mathbf{P}(A) = \sum_{x \in A} \mu(x)$.

If $A, B \subseteq X$, then $\mathbf{P}(A \cup B) \leq \mathbf{P}(A) + \mathbf{P}(B)$. 
Let $F : \mathbf{X} \rightarrow \mathbb{R}^+$. $F$ can be seen as a \textit{random variable} with the distribution $\mu$.

The \textit{mean} of $F$ is $E(F) = \sum_{x \in \mathbf{X}} \mu(x)F(x)$.

$E$ is linear: $E(F + F') = E(F) + E(F')$. This holds even if $F$ and $F'$ are not independent.

If $F(\mathbf{X}) \subseteq \{0, 1\}$, then $E(F) = P(F = 1)$.

If $A \subseteq \mathbf{X}$, then let $\chi_A$ be its characteristic function. Then $E(\chi_A) = P(A)$.

If $F(\mathbf{X}) \subseteq \mathbb{N}$, then $E(F) \geq P(F > 0)$. 
Lemma (Markov’s inequality). Let $F$ be a random variable and $a > 0$. Then

$$\Pr(F \geq a) \leq \frac{\mathbb{E}(F)}{a}.$$ 

Proof.

$$\mathbb{E}(F) = \sum_{x \in X} \mu(x) F(x) \geq \sum_{x \in X \atop F(x) \geq a} \mu(x) F(x) \geq \sum_{x \in X \atop F(x) \geq a} \mu(x) a = \Pr(F \geq a) \cdot a.$$ 

This inequality is helpful for showing that $\Pr(F < a)$ is large.
Let $p \in [0, 1]$. Define the following probability distribution $\mathcal{G}(n, p)$ on the set $G_n$ of $n$-vertex labeled graphs:

Picking $G$ according to $\mathcal{G}(n, p)$ (denote $G \leftarrow \mathcal{G}(n, p)$) proceeds as follows:

- $V(G) := \{v_1, \ldots, v_n\}$. Let $E(G) := \emptyset$.
- For all $i \in \{1, \ldots, n - 1\}$ and $j \in \{i + 1, \ldots, n\}$:
  - Toss a coin, where the probability of heads is $p$.
  - If the result was heads, then $E(G) := E(G) \cup \{(v_i, v_j)\}$.
  - The coin-tosses must be mutually independent.

In the following denote $q = 1 - p$. 
Example. Picking an (unlabeled) graph according to $\mathcal{G}(3, p)$ gives us the following graphs with the following probabilities:

\[ E(\Delta) = 3pq^2 + 6p^2q + p^3. \] If $p = q = 1/2$, then $E(\Delta) = 5/4.$
Let $G \leftarrow \mathcal{G}(n, p)$. Let $H$ be a fixed graph with $n' \leq n$ vertices and $m'$ edges.

Let $\psi : V(H) \rightarrow V(G)$ be an injective function. The probability that $\psi$ locates a copy of $H$ as a subgraph of $G$, is $p^{m'}$.

The probability that $\psi$ locates an induced subgraph $H$ of $G$ is $p^{m'}q^{\left(\frac{n'}{2}\right)-m'}$.

In general, $\Pr(H \leftarrow G) \leq \sum_{U \subseteq V(G)} \Pr(H \cong G[U])$.

This sum is the average number of times $H$ occurs in $G$ as an induced subgraph.
Lemma. Let $G \leftarrow \mathcal{G}(n, p)$. The average number of $k$-vertex cliques in $G$ is $\binom{n}{k}p^{\binom{k}{2}}$ and the average number of $k$-vertex independent sets is $\binom{n}{k}q^{\binom{k}{2}}$.

Proof. Fix $U \subseteq V(G)$, such that $|U| = k$. The probability that $U$ is a clique is $p^{\binom{k}{2}}$.

The average number of cliques in position $U$ is $p^{\binom{k}{2}}$. There are $\binom{n}{k}$ possible positions, and we can just add the averages. 

Let $\alpha(G)$ be the size of the largest independent set that $G$ contains. Then $P(\alpha \geq k) \leq \binom{n}{k}q^{\binom{k}{2}}$.

Recall that $\chi(G) \geq n/\alpha(G)$, where $n$ is the number of vertices of $G$. 
Denote
\[(n)_k = n(n - 1)(n - 2) \cdots (n - k + 1) .\]

**Lemma.** Let \( G \leftarrow G(n, p) \). The average number of cycles of length \( k \geq 3 \) in \( G \) is \( p^k (n)_k / 2k \).

**Proof.** A cycle of length \( k \) is determined by a sequence \((v_1, v_2, \ldots, v_k)\) of different vertices of \( G \).

Such a sequence can be chosen in \((n)_k\) different ways. Each cycle corresponds to \( 2k \) such sequences.

The probability that \( G \) contains the edges \((v_1, v_2), (v_2, v_3), \ldots, (v_{k-1}, v_k), (v_k, v_1)\) is \( p^k \). \qed
Let $X_k(G)$ be the number of cycles of length at most $k$ in the graph $G$. If $G \leftarrow \mathcal{G}(n,p)$, then

$$E[X_k] = \sum_{i=3}^{k} \frac{(n)^i}{2i} p^i \leq \frac{1}{2} \sum_{i=3}^{k} n^i p^i \leq \begin{cases} \frac{k-2}{2} n^k p^k, & \text{if } np \geq 1 \\ \frac{k-2}{2n^3 p^3} \cdot \frac{1}{1-np}, & \text{if } np < 1 \end{cases}$$

This is an upper bound for $P(g \leq k)$. 
To show the existence of a graph $G$ with $g(G) \geq k$ and $\chi(G) \geq k$ we could try to fix $n$ and $p$ so, that

$$P(g \leq k - 1) + P(\alpha \geq n/k) < 1.$$ 

It turns out that there are no such $n$ and $p$...
We will show that we can fix $n$ and $p$ so, that

- $P(X_k \geq n/2) < 1/2$;
- $P(\alpha \geq n/2k) < 1/2$.

We fix $p$ as a function of $n$ so, that both of those probabilities approach 0 if $n \to \infty$.

Hence there exists an $n$-vertex graph $G$ containing less than $n/2$ cycles of length $\geq k$, and no independent set of size $n/2k$. Let $H$ be a graph obtained from $G$ by removing one vertex from each of those short cycles.

$|V(H)| > n/2$. Obviously $g(H) > k$ and $\alpha(H) < n/2k < |V(H)|/k$. Hence $k$ colours are not sufficient to colour $H$. 
Fix $\varepsilon \in \mathbb{R}$, such that $0 < \varepsilon < 1/k$. Let $p = n^{\varepsilon-1}$. Then $0 < p \leq 1$.

\[
P(X_k \geq n/2) \leq \frac{\mathbb{E}[X_k]}{(n/2)} \leq \frac{k-2}{2 \cdot (n/2)} n^k p^k = (k - 2)(np)^k/n = (k - 2)n^{k\varepsilon-1}
\]

- because $np = n^\varepsilon \geq n^0 = 1$.

As $k\varepsilon - 1 < 0$, the above expression tends to 0 if $n \to \infty$. 
Let $r$ be such, that $n \geq r \geq n/2k$.

Note that $p \geq (6k \ln n)/n$ if $n$ is large enough.

$$P(\alpha \geq r) \leq \binom{n}{r}q^{(r)} \leq n^r q^{r(r-1)/2} = (nq^{(r-1)/2})^r \leq \left(ne^{-p(r-1)/2}\right)^r = \left(ne^{-pr/2+p/2}\right)^r \leq \left(ne^{-(3/2)\ln n+p/2}\right)^r \leq \left(nn^{-3/2}e^{1/2}\right)^r = \left(e/n\right)^{r/2}.$$

- because $1 - p \leq e^{-p}$ if $0 \leq p \leq 1$
- because of the lower bounds on $r$ and $p$

If $n \to \infty$, then $e/n \to 0$ and $r/2 \to \infty$. Hence the whole expression tends to 0. □
Let us now consider simple graphs with countably many vertices. In particular, consider graphs distributed according to $G / N$, $B / C$, $D / N$, $B / D$, $B / E$, $B / D$. 

**Theorem.** Let $G_1 \leftarrow \mathcal{G}(\mathbb{N}, 1/2)$ and $G_2 \leftarrow \mathcal{G}(\mathbb{N}, 1/2)$, where $G_1$ and $G_2$ are two independent random variables. Then the following event occurs with probability 1:

There exists an isomorphism from $G_1$ to $G_2$.

In other words, there exists exactly one random countably infinite simple graph.
Consider the following property (*), that a graph $G = (V, E)$ may or may not satisfy:

- for any finite $U, W \subseteq V$, where $U \cap W = \emptyset$

- exists $z \in V \setminus (U \cup W)$

- such that
  - for all $u \in U$, $(u, z) \in V$;
  - for all $w \in W$, $(w, z) \not\in V$. 
Lemma. Let $G \leftarrow \mathcal{G}(\mathbb{N}, 1/2)$. Then $G$ satisfies (*) with probability 1.

Proof. Fix $U$ and $W$. If we also fix $z$, then the probability of (*) holding is $1/2^{|U|+|W|}$. We have infinitely many choices for $z$, thus the probability of (*) holding for some choice of $z$ is 1. \qed
Lemma. Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two countably infinite simple graphs that satisfy (*). Then $G_1 \cong G_2$.

Proof. Identify both $V_1$ and $V_2$ with $\mathbb{N}$.

We construct the isomorphism $\varphi : V_1 \to V_2$ in rounds.

- In the beginning, $\varphi$ is everywhere undefined. Each round defines $\varphi$ for one element of $V_1$ (and $V_2$).

- For any $v_1 \in V_1$, $\varphi(v_1)$ will be defined after a finite number of rounds.

- For any $v_2 \in V_2$, $\varphi^{-1}(v_2)$ will be defined after a finite number of rounds.

After countably many rounds, we have a uniquely defined bijection between $V_1$ and $V_2$. It will be an isomorphism.
\textit{n}-th round (for odd $n$):

- Let $x_n = \min\{x \in V_1 \mid \varphi(x) \text{ is undefined}\}$.
- Let $U_n = \{v \in V_1 \mid (x_n, v) \in E_1 \land \varphi(v) \text{ is defined}\}$.
- Let $W_n = \{v \in V_1 \mid (x_n, v) \not\in E_1 \land \varphi(v) \text{ is defined}\}$.
- By (*) for $G_2$, there exists some $y_n \in V_2 \setminus (\varphi(U_n) \cup \varphi(W_n))$, such that $y_n$ is connected to all vertices in \( \varphi(U_n) \) and to no vertices in \( \varphi(W_n) \).
  - \( \varphi^{-1} \) is defined only for vertices in \( \varphi(U_n) \cup \varphi(W_n) \),
  - hence \( \varphi^{-1}(y_n) \) is not defined.
- Let the new value of $\varphi$ be $\varphi[x_n \mapsto y_n]$. 
$n$-th round (for even $n$) (just swap $G_1$ and $G_2$):

- Let $y_n = \min\{y \in V_2 \mid \varphi^{-1}(y)$ is undefined\}.
- Let $U_n = \{v \in V_2 \mid (y_n, v) \in E_2 \land \varphi^{-1}(v)$ is defined\}.
- Let $W_n = \{v \in V_2 \mid (y_n, v) \not\in E_2 \land \varphi(v)$ is defined\}.
- By (*) for $G_1$, there exists some $x_n \in V_1 \setminus (\varphi^{-1}(U_n) \cup \varphi^{-1}(W_n))$, such that $x_n$ is connected to all vertices in $\varphi^{-1}(U_n)$ and to no vertices in $\varphi^{-1}(W_n)$.
  - $\varphi$ is defined only for vertices in $\varphi^{-1}(U_n) \cup \varphi^{-1}(W_n)$,
  - hence $\varphi(x_n)$ is not defined.

- Let the new value of $\varphi$ be $\varphi[x_n \mapsto y_n]$. $\square$

From those two lemmas, the theorem immediately follows. $\square$