Combinatorics, 2016 Fall, USTC

Week 12, November 24

Ramsey's Theorem

Recall:

- $R(s,t) \leq \binom{s+t-2}{s-1}$, $s.t \geq 2$.
- $R(s,t) \leq R(s-1,t) + R(s,t-1)$.

Theorem 1. *If for some (s,t), the numbers $R(s-1,t)$ and $R(s,t-1)$ are even, then*

$$R(s,t) \leq R(s-1,t) + R(s,t-1) - 1.$$

Proof. Let $n = R(s-1,t) + R(s,t-1) - 1$. So n is odd. Consider any 2-edge-coloring of K_n. For any vertex x, define $Bx = \{y : xy \text{ is blue.}\}$ and $Rx = \{y : xy \text{ is red.}\}$.

If $\exists v$ s.t. $|Bv| \geq R(s-1,t)$ or $|Rv| \geq R(s,t-1)$, then by the definition of Ramsey number, we can find a blue K_s or a red K_t. Thus, we may assume, for any vertex v, $|Bv| \leq R(s-1,t) - 1$ and $|Rv| \leq R(s,t-1) - 1$.

But $n - 1 = |Bv| + |Rv| \leq R(s-1,t) + R(s,t-1) - 2 = n - 1$. This implies that for each v, $|Bv| = R(s-1,t) - 1$ is odd. This shows that the graph G consisting of all blue edges has odd number of vertices, where each vertex is of odd degree in G. But this contradicts the Handshaking Lemma. ∎

Definition 2. For any $k \geq 2$ and integers $s_1, s_2, ..., s_k \geq 2$, the Ramsey number $R_k(s_1, s_2, ..., s_k)$ is the least integer N such that any k-edge-coloring of K_N has a clique K_{s_i} in color i, for some $i \in [k]$.

Homework. $R_k(s_1, s_2, ..., s_k) < +\infty$.

Theorem 3 (Schur's Theorem)**.** *For $k \geq 2$, there exists some integer $N = N(k)$ such that any coloring $c : [N] \to [k]$ contains $x, y, z \in [N]$ satisfying that $c(x) = c(y) = c(z)$ and $x + y = z$.*

Proof. Let $N = R_k(3, 3, ..., 3)$. Define a k-dege-coloring of K_N. From the coloring c as following: $\forall i, j \in [N]$, define the color of ij to be $c(|i - j|)$. By the choice of N, we see that there exists a monochromatic K_3, say ijl, where $i < j < l$. Let $x = j - i$, $y = l - j$, and $z = l - i$. Then $c(x) = c(y) = c(z)$ and $x + y = z$. ∎

Using this theorem, Schur proved that Fermat last Theorem holds in $\mathbb{Z}_p$ for sufficiently large prime p.

Theorem 4. *For any integer $m \geq 1$, there is a prime $p(m)$ s.t. for any prime $p \geq p(m)$, $x^m + y^m = z^m$ (mod p) has a nontrivial solution.*

Proof. For prime p, consider the multiplicative group $\mathbb{Z}_p^*$. Let g be a generator of $\mathbb{Z}_p^*$. Then $\forall x \in \mathbb{Z}_p^*$, there exists exactly one pair of integers (i, j) s.t. $0 \leq j \leq m - 1$, $0 \leq im + j \leq p - 2$ and $x = g^{im+j} \pmod p$, since $\mathbb{Z}_p^*$ is a cyclic of order $p - 1$.

We then can define a function $c : \mathbb{Z}_p^* \to \{0, 1, ..., m-1\}$ by letting $c(x) = j$, where $x = g^{im+j}$ and $0 \leq j \leq m - 1$.

By Schur's Theorem, choose $p(m) = N(m)$, so for any $p \geq p(m)$, the function c has $x, y, z \in \mathbb{Z}_p^*$ s.t. $c(x) = c(y) = c(z)$ and $x + y = z$. Let $x = g^{i_1 m+j}$, $y = g^{i_2 m+j}$, $z = g^{i_3 m+j} \pmod p$.

Then $x + y = z$.

$$\Rightarrow g^{i_1 m+j} + g^{i_2 m+j} = g^{i_3 m+j} \pmod p \tag{1}$$

$$\Rightarrow g^{i_1 m} + g^{i_2 m} = g^{i_3 m} \pmod p.$$

Let $\alpha = g^{i_1},\ \beta = g^{i_2},\ \gamma = g^{i_3}$,

$$\Rightarrow \alpha^m + \beta^m = \gamma^m \pmod p.$$

∎

Remark. Schur's Theorem holds in $\mathbb{Z}$, but we need to restrict the calculation into a multiplication cyclic group when deducing equation (1).

Theorem 5. *Let n, s satisfy $\binom{n}{s} \cdot 2^{1-\binom{s}{2}} < 1$. Then $R(s,s) > n$.*

Proof. We need to construct a 2-edge-coloring of K_n which has NO monochromatic K_s.

(To be continued.) ∎